Takács Gergely

KIBERTERRORIZMUS – VOLT, VAN, LESZ? LÉTEZNEK-E FEHÉRGALLÉROS DZSIHÁDISTÁK?[1]

BEVEZETÉS

A kétezres évek elején a kiberterrorizmussal mint fenyegetéssel széleskörűen foglalkozott a média, a politikai, a biztonsági és a rendvédelmi szféra is, és olyan forgatókönyveket vázoltak fel, amelyekben képzett kiberterroristák kritikus (információs) infrastruktúrák rendszereibe törnek be és okoznak akár több millió embert érintő károkat, vagy esetleg személyi sérüléseket is. Ezen szcenáriók közül egyik sem valósult meg egészen a napjainkig. Ebből adódóan fontos feltenni a kérdést, hogy egyáltalán mennyire tekinthető valós fenyegetésnek a kiberterrorizmus? Figyelembe véve a digitalizáció, digitális transzformáció trendjeit és azt, hogy az infokommunikációs technológiák a modern társadalmak és gazdaságok működésének elengedhetetlen elemévé váltak, a félelem akár jogos is lehet. Már csak azért is, mert napi rendszerességgel jelennek meg azzal kapcsolatos hírek, hogy hackerek milyen, kritikus infrastruktúrának számító rendszereket támadtak meg és jutottak be sikeresen. Tehát a terroristák akár meg is tehetnék, hogy a kiberbűnözők és államok által támogatott hackercsoportok módszereit követve, azokat a darkneten megvásárolva vagy lemásolva hozzáférést szerezzenek a kormányzati, katonai, pénzügyi vagy egészségügyi rendszerekhez, és megpróbáljanak valamilyen mértékű kárt okozni.

A kiberterrorizmustól való félelmet sokáig az fűtötte, hogy a fizikai terrortámadások a nyugati szövetségi rendszer tagjai, szervezetei, intézményei, multinacionális vállalatai ellen gyakorlatilag folyamatosak voltak az 1990-es évek végétől egészen az elmúlt évekig. Emellett a kibertér biztonságával kapcsolatban is folyamatosan születtek a különböző stratégiai dokumentumok és politikai deklarációk, amelyekben a fenyegetések felsorolásában mindig helyet kapott a kiberterrorizmus is. Emellett az európai és amerikai hírszerző közösség tagjai által készített éves jelentések alapján is elmondható, hogy a kiberterrorizmus, pontosabban annak egyes

[1] Az indiai rendőrség által használt kifejezés, amikor 2021-ben letartóztattak öt hackert, akik támadást terveztek újságírók, társadalmi aktivisták, ügyvédek és politikai funkcionáriusok ellen, hogy félelmet keltsenek a társadalomban. *Jammu and Kashmir Police cracking down on white-collar jihadis* 2021.

DOI: https://doi.org/10.36250/01259_17

típusai továbbra is jelen vannak, és közvetve vagy közvetlenül szerepet játszanak merényletek elkövetésében.

Jelen tanulmánynak nem célja, hogy számos magyar és külföldi szerzőt követően újfent bemutassa a kiberterrorizmus elméleti hátterével kapcsolatos ismereteket, és nem kíván állást foglalni az ezen bűncselekmény-kategória megítélése kapcsán kialakult jogi, szakértői viták tekintetében sem. Helyette arra keresi a választ, hogy eddig miért nem került sor olyan jellegű, a kibertérben végrehajtott támadásra, amely a kritikus infrastruktúrák ellen irányult volna működésük tömeges, széles körű elszabotálása, megzavarása érdekében.

A kockázatok meglétének elismerése ellenére a dolgozat nem kíván foglalkozni a kibertér azon „soft" jellegű terroristák általi felhasználásával, amely a propaganda terjesztésére, tagok toborzására, pénzügyi források előteremtésére koncentrál. Helyette a Dorothy E. Denning[2] által megfogalmazott kiberterrorizmus definíciót kívánja alapul venni. Denning szerint a kiberterrorizmust a kibertér és a terrorizmus konvergenciájaként lehet értelmezni. Ennek megfelelően a kiberterrorizmus számítógépek, hálózatok és az azokon tárolt információk elleni jogellenes támadásokat és támadással való fenyegetést jelenti egy kormány vagy az ország lakosságának megfélemlítése céljából, az elkövetők által elérni kívánt politikai vagy társadalmi változás előmozdítása érdekében. Ahhoz, hogy kiberterrorizmusnak minősüljön egy cselekmény, a támadásnak személyek vagy tulajdon elleni erőszakot kell eredményeznie, vagy legalábbis olyan kárt kell okoznia, amely félelmet kelt. A kritikus infrastruktúrák elleni súlyos támadások hatásuktól függően számíthatnak kiberterrorizmusnak vagy egyéb bűncselekménynek. Az olyan támadások, amelyek nem létfontosságú szolgáltatásokat zavarnak meg, vagy amelyek elsősorban költséges „kellemetlenséget" okoznak, a kiberterrorizmus Denning által megalkotott fogalmi keretén kívülre kerülnek.

KIBERTERRORIZMUS – MIÉRT ÉS MIRE JÓ?

A technológia folyamatos fejlődése és elterjedése a fenyegetések új kategóriáját, a kiberfenyegetéseket hozta létre, amelyekkel a társadalmaknak szembe kell nézniük. Ezek a kiberfenyegetések általánosságban úgy határozhatók meg, mint a különböző informatikai eszközök felhasználása olyan tevékenységre, amely alááshatja a társadalom belső vagy külső rend fenntartására irányuló képességét.

[2] DENNING 2001.

Történelmileg a társadalmak Susan W. Brenner[3] meglátása szerint kétirányú stratégiát alkalmaztak a túléléshez és a jóléthez szükséges rend fenntartására: a belső rendet olyan előíró szabályok megfogalmazásával és érvényesítésével tartják fenn, amelyek révén igyekeznek megakadályozni, hogy a társadalom tagjai széles körben aláássák azt. A társadalmak a külső rendet a katonai erőre és egyre nagyobb mértékben nemzetközi megállapodásokra támaszkodva tartják fenn.

A technológiai fejlődés következtében megkérdőjeleződnek a belső és külső rend fenntartásának ezen törvényszerűségei. A hagyományos megközelítés feltételezi, hogy a társadalmak területileg meghatározott földrajzi adottságok között élnek, amelyben a fenyegetések könnyen azonosíthatók belső (például bűnözés) vagy külső (például háború) fenyegetésekként. Az infokommunikációs technológiák és a digitális transzformáció megkérdőjelezi ennek a feltételezésnek az érvényességét is, mivel a területi megközelítést egyre kevésbé teszi relevánssá. A hálózatok, rendszerek, iparágak, kereskedelmi kapcsolatok összekötöttségéből fakadóan a szigetszerűen működő országok gyakorlatilag megszűntek. A 21. században azok, akik arra törekszenek, hogy aláássák egy társadalomnak ezt a rendfenntartó képességét, a kibertér segítségével képesek támadásokat indítani a világ szinte bármely pontjáról.

Ahhoz, hogy megértsük, mi tekinthető kiberterrorizmusnak, meg kell vizsgálni, hogyan használhatják a terroristák az informatikai eszközöket a civil lakosság megfélemlítésére vagy kényszerítésére, a társadalmi rend megbontására. Brenner három kategóriát alkotott meg.[4]

- *Tömeges pusztítás fegyvere:*[5] az első kategóriába tartozó támadásoknak egyelőre csak elméleti valószínűsége létezik, hiszen azt feltételeznék, hogy kizárólag számítógépek segítségével az amerikai (New York, Boston) vagy európai (Madrid, London, Nizza) terrortámadásokhoz hasonló merényletek végrehajtására nyílna lehetőség.
- *Tömeges megtévesztés fegyvere:*[6] a közrend/fegyelem megzavarása tömeges megtévesztés révén egyszerre elméleti és reális lehetőség is. Ebben az esetben is központi szerepet játszanak az informatikai eszközök egy terrorista cselekmény elkövetésében azáltal, hogy a számítógépes technológiát a polgári lakosság pszichológiai manipulálására használják fel. A pszichológiai befolyásolás (például pánikkeltés, tömeghisztéria kiváltása) típusától függően személyi sérülések, halálesetek és vagyoni károkozás is előfordulhat, de erre sem volt még eddig precedens.

[3] Brenner 2006.
[4] Brenner 2006: 458–461.
[5] Weapon of mass distruction.
[6] Weapon of mass distraction.

- *Tömeges megzavarás fegyvere:*[7] a számítástechnika – különböző rendszerek működésének – tömeges megzavarásra való felhasználásával a terroristák célja, hogy aláássák a civil lakosságnak az olyan infrastrukturális elemek stabilitásába és megbízhatóságába vetett hitét, mint a tömegközlekedés, az áramszolgáltatás, a telekommunikáció, a pénzintézetek és az olyan létfontosságú szolgáltatások, mint az egészségügyi ellátás. Látható, hogy a kettes és hármas kategória között hasonlóság van, ugyanakkor fontos különbség, hogy a számítástechnikát hogyan használják fel a civil lakosság társadalmi infrastruktúrába és intézményekbe vetett bizalmának megingatására. A tömeges megzavarás lényege a pszichológiai manipuláció, amihez az infokommunikációs eszközöket használják fel, de nem előfeltétele a rendszerek tényleges megtámadása.

A modern terroristák szempontjából a kiberterrorizmus jó alternatíva lehet, mert olcsóbb a hagyományos terrorista módszereknél, ráadásul nem kellenek hozzá olyan eszközök, amelyek felkelthetik a rendvédelmi, nemzetbiztonsági szervek érdeklődését – ellentétben a robbanóanyagokkal és prekurzorokkal,[8] amelyek folyamatos monitoring alatt vannak. A kiberterrorizmus által biztosított anonimitásnak is nagy előnye van, igaz, itt csak az elkövetők személyére kell gondolni, hiszen amennyiben a kiberterrorista támadást egyik szervezet sem vállalja magára, akkor pont a deklarálni kívánt ideológiai/vallási/politikai célból történő figyelemfelkeltés marad el. A fizikaival szemben a kibertérben nincsenek határok, ellenőrz ő pontok, és nem kell számítani a rendvédelmi szervek munkatársaira sem. A potenciális célpontok száma exponenciálisan megnő a kibertérben. A potenciális célpontok puszta száma és összetettsége garantálja, hogy a terroristák megtalálják a kihasználható gyenge pontokat és sebezhetőségeket. A kiberterrorista cselekmények távolról is végrehajthatók, kevesebb fizikai előkészület, pszichológiai felkészítés és utazás kell hozzá, kisebb az elkövető elhalálozásának esélye, és mindezen „előnyöket" figyelembe véve végső soron megkönnyíti a terrorista szervezetek számára a toborzást is. A kiberterrorizmus révén megvan az esély arra, hogy a fizikai támadásokhoz képest nagyobb számú érintettre gyakoroljanak vele hatást, és ezáltal nagyobb médialefedettséget érjenek el.

Amennyiben Denning kiberterrorizmussal kapcsolatos definícióját vesszük alapul, akkor a támadók esetében fontos, hogy a Plotnek és Slay[9] által meghatározott hat ismérv mindegyike teljesüljön. Minden más esetben ugyanis már a kiberhadviselés

[7] Weapon of mass disruption.

[8] Kábítószerek és pszichotróp anyagok tiltott előállítása során felhasznált vegyi anyagok.

[9] Plotnek–Slay 2021.

vagy a kiberbűnözés, vagy éppen a hacktivizmus[10] területére tévednénk át.[11] Attribútumok:

- az elkövető(k): nem állami, terrorista szervezet, és titokban szervezik a tevékenységüket;
- motiváció: lehet politikai, társadalmi, gazdasági vagy ideológiai;
- szándék: valamely intézkedés, cselekvés előidézésének vagy kikényszerítésének szándéka, változás előidézése, célok előmozdítása vagy zavar okozása;
- eszközök: a bűncselekmény elkövetésének módszere, amely magában foglalja a számítógép és a hálózat használatát a kibertérbe való bejutáshoz, a kiberhadviselés vagy kiberbűncselekmény kategóriájába tartozó tevékenységekkel támadás végrehajtása, fenyegetés gerjesztése;
- hatás: erőszak, szolgáltatásmegszakítások, fizikai károkozás, pszichoszociális károk, gazdasági veszteségek vagy adatszivárogtatás;
- célpont: jellemzően civilek, infokommunikációs technológia, adatforrások, kormányzati intézmények, nem kormányzati szervezetek, fizikai infrastruktúra támadása.

A kiberterrorizmus irányulhat információs infrastruktúrák, fizikai gépek elpusztítására, az internetes, kormányzati informatikai hálózatok, polgári kritikus rendszerek (pénzügyi szektor, média) működésének távolról történő megzavarására. A kiberterrorista szervezetek célja, hogy széles körű zűrzavart keltsenek, megzavarják a létfontosságú infrastruktúrát, támogassák a politikai tevékenységet vagy a hacktivizmust, illetve fizikai károkat vagy akár halált okozzanak. Indokoltnak tartom ehelyütt megjegyezni, hogy annak ellenére, hogy a szakirodalom túlnyomó többsége azonos álláspontot képvisel ezen jellemzők vonatkozásában, a tanulmányok, cikkek, kiberbiztonsági cégek elemzései mégis – elsősorban – a kiberhadviselés, kiberbűnözés kategóriájába tartozó eseteket hoznak fel példaként a kiberterrorizmusra. Feltehetően

[10] A hacktivizmus politikai, ideológiai indíttatásból, motivációból elkövetett kibertámadás, hackelés, jellemzően szólásszabadság, emberi jogok és az információ szabadsága melletti kiállás érdekében.

[11] Egyes cikkekben megjelenik egy ötödik kategória is, az úgynevezett kiberharcosok, akik a hacktivisták és a jellemzően valamely totalitárius politikai rendszerek (például iráni, szíriai) nevében kibertámadásokat végrehajtó csoportok keveréke. Ez a kategória némileg vitatható, mert bár egyértelműen nem lehet azt kijelenteni, hogy nemzetállami aktoroknak tekinthetők ezek a kiberharcosok, de az a diktatórikus politikai berendezkedés, amelyben működnek, gyakorlatilag kizárja annak lehetőségét, hogy az állam tudta és engedélye nélkül működjenek.

nem függetlenül attól a ténytől, hogy a Denning által felállított kritériumok alapján a mai napig egyetlen kibertámadás sem volt terrorizmusnak minősíthető.[12]

Leggyakrabban a kiberhadviselés kategóriájához sorolt támadásokat szokták a kiberterrorizmussal „összekeverni". Erre magyarázatként Eugene Kaspersky[13] azt a magyarázatot adta, hogy a kiberhadviselés szót azért nem lehet használni, mert az azt feltételezné, hogy van két ismert szemben álló fél, azonban az esetek többségében nem ez a helyzet. Manapság ugyanis nem lehet megmondani, megállapítani teljes bizonyossággal, hogy ki vagy kik az elkövetői a kormányzati rendszerek, kritikus infrastruktúrák elleni támadásoknak, ezért ez a fajta tevékenység nem tekinthető kiberhadviselésnek. Meglátása szerint a kiszámíthatatlanság és a bizonytalanság (pszichológiája) miatt kell ezt a fajta tevékenységet kiberterrorizmusnak nevezni, ugyanis ezt a pszichózist az váltja ki, hogy nem lehet tudni, ki követte el a támadást, és ha újra támad, akkor mikor és milyen rendszer ellen fogja bevetni a kiberfegyvereit. Kaspersky hasonlóságot lát a biológiai fegyverek és a kiberfegyverek között a tekintetben, hogy bevetésük esetén egyiket sem lehet kontroll alatt tartani. Egy olyan mértékben összekötött, digitalizált világban, amelyben jelenleg élünk, kiszámíthatatlan, hogy a kiberfegyverek milyen sebességgel és milyen irányokba terjednek el. Erre nagyon jó példaként lehet felhozni a NotPetya malware-t, amelyet Ukrajna elleni kibertámadáshoz fejlesztett ki az orosz katonai hírszerzéshez (GRU)[14] köthető Sandworm hackercsoport, de a világ számos pontján megjelent, és rendszerleállásokat okozott.[15]

A számítógépes hackerek és a terroristák vagy a terroristákat támogató országok közötti kapcsolatokat nehéz megerősíteni. A legjobban képzett számítógépes hackercsoportok tagsága néha nagyon exkluzív, és olyan egyénekre korlátozódik, akik a legjobban őrzött, kifinomult hackereszközöket fejlesztik ki, mutatják be, és csak egymással osztják meg. Ezek az exkluzív hackercsoportok nem keresik a figyelmet, mert a titoktartás fenntartása lehetővé teszi számukra a hatékonyabb működést. Egyes hackercsoportoknak nemzetek feletti, szupranacionális, vallási vagy más társadalmi-politikai ideológián alapuló politikai érdekeik is lehetnek, míg más

[12] Ez a kijelentés abból a szempontból nem tekinthető pontosnak, hogy az amerikai büntető törvénykönyv passzusai alapján ítélet is született már kiberterrorizmus vádjával 2016-ban. Az amerikai Igazságügyi Minisztérium vádat emeltetett Ardit Ferizi ellen, aki katonai weboldalakat tört fel, és az onnan ellopott kormányzati és honvédelmi munkatársak személyes adatait, lakcímeit eladta az Iszlám Államnak, hogy terrortámadásokat követhessenek el velük szemben. Blake 2016.

[13] Shamah 2012.

[14] Главное разведывательное управление (Glavnoje razvedivatyelnoje upravlenyije): Felderítő Főcsoportfőnökség.

[15] *Global ransomware attack causes turmoil* 2017.

hackercsoportokat a profit motiválhat, vagy a szervezett bűnözéshez kapcsolódhatnak, és a politikai érdekektől függetlenül hajlandóak lehetnek eladni számítógépes szolgáltatásaikat. Szakértői becslések[16] szerint a több rendszer és hálózat ellen irányuló fejlett vagy strukturált kibertámadások, beleértve a célzott megfigyelést és a kifinomult új hackereszközök tesztelését, akár többéves előkészületet is igényelhetnek, míg egy integrált, heterogén rendszerek elleni, tömeges zavarokat okozó, komplex, összehangolt kibertámadás még ennél is hosszabb felkészülést igényelhet. Ami nem lenne idegen a terrorista csoportoktól, hiszen például az al-Káida által indított korábbi, fizikai térben végrehajtott terrortámadásokat és robbantásokat is több esetben hosszas előkészítés és tervezés előzte meg. Ugyanakkor nehéz meghatározni a nemzetközi terrorista csoportok érdeklődésének szintjét vagy képességeit egy hatékony kibertámadás indítására. Ráadásul a kiberterroristáknak egyszerre több célpontot kellene megtámadniuk hosszú időn keresztül ahhoz, hogy folyamatosan fenyegetést jelentsenek, stratégiai céljaikat elérjék, vagy egyáltalán bármilyen észrevehető hatást gyakoroljanak a nemzetbiztonságra és/vagy a nemzetgazdaságra.

Ennek abból a szempontból van jelentősége, hogy a legtöbb kritikusinfrastruktúra-ágazat (például az elektromos hálózatot kezelő vállalatok) működését felügyelő, szabályozó és irányító SCADA-rendszerekhez,[17] illetve az ipari vezérlőrendszerekhez (ICS)[18] való hozzáférés megszerzése, esetleg az irányítás átvétele egyre összetettebb, nagy szakértelmet és sok ráfordított időt igénylő feladattá vált, annak ellenére, hogy sok SCADA-rendszer ma már a kereskedelmi forgalomban kapható szoftverekkel működik, amelyek gyakran nem rendelkeznek megfelelő védelemmel a kibertámadások ellen. Igaz, ebben a tekintetben jelentős változások voltak az elmúlt években mind az Egyesült Államokban, mind az Európai Unió területén.[19]

Amennyiben adottnak vesszük, hogy a kritikus infrastruktúrák sebezhetők egy kiberterrorista támadással szemben, akkor a kérdés az, hogy vannak-e olyan szereplők, akik képesek és motiváltak egy ilyen művelet végrehajtására. Bár egyre több hacker rendelkezik a számítógépes rendszerek megtámadásához szükséges ismeretekkel,

16 Wilson 2008.

17 Supervisory control and data acquisition – felügyeleti ellenőrző és adatgyűjtő rendszer, amely az érzékelők által gyűjtött digitalizált visszacsatolási adatok alapján automatikusan felügyeli és szabályozza a kapcsolási, gyártási és egyéb folyamatszabályozási tevékenységeket. Ezeket az ellenőrző, ipari vezérlőrendszereket gyakran távoli helyeken helyezik el, személyzet nélküliek, és interneten keresztül férnek hozzájuk a mérnökök a nagyobb hatékonyság érdekében.

18 Industrial Control System.

19 A kritikus (információs) infrastruktúrák védelme érdekében az USA-ban számos elnöki rendelet és kiberbiztonsági szabvány került elfogadásra, hasonlóan az EU-hoz, ahol az uniós intézmények több regulatív intézkedést is meghoztak a társadalom és a gazdaság működése szempontjából létfontosságúnak számító ágazatok kiberbiztonsági szintjének fejlesztésére.

készségekkel és eszközökkel, általában nincs meg bennük a motiváció arra, hogy erőszakot vagy súlyos gazdasági, társadalmi károkat okozzanak. Ezzel szemben úgy tűnik, hogy az erőszakra motivált terroristáknak nincs meg a képességük vagy a motivációjuk arra, hogy ilyen mértékű kárt okozzanak a kibertérben. Az amerikai haditengerészet Montereyben, Kaliforniában található posztgraduális iskolájának munkatársai[20] által készített tanulmány három kategóriát különített el az alapján, hogy egy kiberterrorista csoport milyen képességekkel rendelkezhet.

- *Egyszerű-strukturálatlan:* Olyan mértékben rendelkeznek képességekkel, hogy valaki más által létrehozott eszközök segítségével alapvető hackeléseket végre tudnak hajtani egyes rendszerek ellen. Szaktudás hiányában a módszereik jellemzően az egyszerű próbálkozásokon alapulnak, a támadások nem célzottak, előzetes felderítés nem előzi meg az akciókat, amelyek jellemzően weboldalak elérhetetlenné tételében vagy tartalmának az üzemeltető szándékai ellenére történő megváltoztatásában (deface-elésében) merülhetnek ki. Az ebbe a kategóriába sorolt szervezet minimális parancsnoki és vezetési, illetve tanulási képességgel rendelkezik.
- *Fejlett-strukturált:* A szervezet képes több rendszer vagy hálózat ellen bonyolultabb támadásokat végrehajtani, és esetleg alapvető hackereszközöket módosítani vagy akár már létrehozni is. A szervezet elemi célpontelemzési, parancsnoki és irányítási, valamint tanulási képességgel rendelkezik, ezáltal lehetővé válik, hogy ugyanabból az irányból, de sorozatosan hajtsanak végre támadásokat. A célpontelemzés azon a szinten van, hogy képesek felderíteni a támadott rendszer konfigurációját, szoftverkörnyezetét. A támadás közvetlen hatásaival valószínűleg tisztában vannak, de a potenciális kaszkádhatásokat biztosan nem mérik fel előzetesen. A fejlett-strukturált kiberterrorista szervezetek tevékenységének eredménye támogatásul szolgálhat a hagyományos terrorista műveleteknek. A fejlett-strukturált szervezetek tagjai képesek tanulni és új technológiákat elsajátítani, tisztában vannak vele, hogy ez elengedhetetlen a fejlődésükhöz. A tanulás révén a kiberterrorista csoportból a lehetőséget, a szükséges feltételeket megteremtő szervezet válhat.
- *Komplex-koordinált:* Összehangolt, tömeges meghibásodást okozó támadások végrehajtása integrált, heterogén védelemmel rendelkező rendszerek ellen. Az ezen a fejlettségi fokon lévő kiberterrorista csoportok képesek kifinomult hackereszközök létrehozására, a célpontok/rendszerek elemzésére, parancsnoki és vezetési rendszer kialakítására, valamint szervezeti tanulásra. Ez utóbbi képesség lehetővé teszi, hogy naprakész technológiai

[20] Nelson 1999.

> tudással rendelkezzenek a hackerek, a vezetési-parancsnoki rendszer pedig azt, hogy egyszerre sok célpont ellen indítsanak támadást. A komplex koordinált csoportok fejlett felderítési, információszerzési és elemzési képességekkel rendelkeznek a támadni kívánt rendszerekről. Ez egyúttal azt is feltételezi, hogy tevékenységüket a kezdeti fázisban fedetten, észrevétlenül tudják végrehajtani, és az így megszerzett információk alapján fejlesztik ki a támadni kívánt rendszerekhez leginkább megfelelő szoftvereket.[21]

Az 1999-ben publikált tanulmány becslései szerint egy teljesen az alapokról induló csoportnak 2–4 évbe telik, hogy elérje a fejlett struktúrájú szintet, és 6–10 évbe, hogy elérje a komplex-koordinált szintet, bár egyes csoportok akár néhány év alatt is elérhetik ezt az „érettséget", vagy kiszervezéshez vagy szponzoráláshoz folyamodhatnak, hogy kiterjesszék képességeiket. Figyelembe véve a hackeléshez használatos eszközökhöz való hozzáférés napjainkra kialakult lehetőségeit, a képességek megszerzéséhez szükséges idő lerövidülhetett, igaz, a szervezetként való koordinált működés feltételeinek megteremtése továbbra is időigényesnek bizonyulhat.

A KIBERTERRORIZMUS – VALÓS KOCKÁZATOK

A kiberterrorizmus által jelentett tényleges kockázat hozzávetőleges felvázolhatósága érdekében a forrásként felhasznált cikkeken és tanulmányokon kívül áttekintésre kerültek az amerikai hírszerző közösség által 2006 és 2023 között évente összeállított fenyegetettségi elemzések[22] is. A továbbiakban ennek az eredményeit kívánom ismertetni. A jelentések alapján látható, hogy kiberfenyegetés – annak ellenére, hogy már a 2001. szeptember 11-i terrortámadást megelőzően is valós szcenárióként kezelték – semmilyen vonatkozásban nem jelent meg sem a 2006-os,[23] sem

[21] NELSON et al. 1999: 13–17.

[22] Annual Threat Assessment of the U.S. Intelligence Community. Office of the Director of National Intelligence (DNI, 2019-től ODNI). A kiválasztás okai között meg kell említeni, hogy kizárólag ezen elemzéseket volt lehetőség historikusan ilyen hosszú időre visszamenőlegesen is áttekinteni. Mivel az éves elemzések valamennyi fenyegetést számba vették, össze lehetett hasonlítani a többi fenyegetéstípussal (például szervezett bűnözés, kémkedés, gazdaságbiztonság), hogy azokhoz képest mekkora kockázatot jelent, és le lehetett mérni azt is, hogy a kiberfenyegetéseken belül milyen hangsúlyosan van jelen a terrorizmus. Meglátásom szerint ebből a két dologból lehetett következtetést levonni: egyrészt az éves jelentésen belül elfoglalt helye (hányadik fejezet foglalkozott az adott témával), másrészt a terjedelme.

[23] Director of National Intelligence 2006.

a 2007-es[24] elemzésekben. A 2008-as kiadásban[25] a fenyegetések között megjelentek az ellenséges kibertámadások, amelyeknek száma folyamatosan növekszik, az elkövetőik között pedig kormányokat, nem állami szereplőket és bűnöző csoportokat említenek meg. A kiberfenyegetések esetében a terrorista csoportokkal összefüggésben említik, hogy az al-Káida, a Hamász és a Hezbollah is kifejezte azon szándékát, hogy a kibertérben is támadásokat kíván végrehajtani az USA ellen, de a képességeikre vonatkozóan – például Oroszországgal, Kínával vagy Iránnal ellentétben – nem közölnek információkat. A 2009-es jelentés[26] az előző évivel szinte szó szerint megegyezett, viszont a 2010-ben kiadottban[27] már volt némi változás, ugyanis abban összefoglalóan azt írják, hogy nemzetállamok, terrorista hálózatok, szervezett bűnözői csoportok, egyének és más kibertényezők próbálnak különböző szofisztikáltságú módszerekkel betörni az amerikai hálózatokba, rendszerekbe. A terrorista csoportok kapcsán azonban továbbra is csak megismétlik a 2008-as fordulatot, amely szerint a kibertér nyújtotta lehetőségeket is ki fogják használni amerikai célpontok és állampolgárok elleni támadások kivitelezésére.

Érdemi változás a 2013. évi jelentésben[28] volt látható két szempontból is. Egyrészt a kiberbiztonsági kockázatok a kritikus infrastruktúrák vonatkozásában megelőzték a terrorizmus jelentette fenyegetéseket. Az elemzésben kitérnek arra, hogy a kevésbé szofisztikált támadások is gondot jelenthetnek, mert még mindig vannak olyan amerikai villamosenergia-hálózatok, amelyek nem rendelkeznek megfelelően magas szintű védelemmel. Ugyanakkor ezeket a lehetőségeket nem biztos, hogy fel tudják majd használni arra, hogy komolyabb ellátási zavarokat okozzanak. Felhívják a figyelmet, hogy látnak arra utaló jeleket, hogy a terrorista szervezetek fokozott érdeklődést mutatnak támadó képességek megszerzése iránt. Egyúttal azonban megjegyzik, hogy amennyiben sikerül is szert tenniük ilyenre, azok korlátozottan lesznek használhatók kritikus infrastruktúrák támadására elsősorban erőforráshiány miatt, másodsorban a terrorista szervezeteken belül konkuráló egyéb feladatokra, célkitűzésekre való tekintettel. A 2014-ben[29] kiadott elemzésben a kiberterrorizmus még eggyel hátrébb sorolódott a fontossági sorrendben a kiberbiztonság és a kémelhárítás mögé. A sorrend és az értékelés nem változott a következő évben[30] sem, kizárólag annyival került kiegészítésre, hogy a terrorista

[24] Director of National Intelligence 2007.
[25] Director of National Intelligence 2008.
[26] Director of National Intelligence 2009.
[27] Director of National Intelligence 2010.
[28] Director of National Intelligence 2013.
[29] Director of National Intelligence 2014.
[30] Director of National Intelligence 2015.

csoportokkal szimpatizálók esetében fennáll a lehetősége annak, hogy alacsony szintű és szofisztikáltságú támadásokat követnek el kizárólag a média figyelmének felkeltése érdekében. A 2016. évi jelentésben[31] a kibertér és a különböző technológiák[32] szerepelnek az első helyen, míg a terrorizmus a másodikon. A kiberterrorizmus kapcsán elsősorban a *soft* kategóriába tartozó kockázatokat emelik ki, mint a propaganda terjesztését, a pénzgyűjtést és a toborzást, valamint az információszerzést az online térben. Fontos megemlíteni, hogy ezekre az évekre tehető az Iszlám Állam kiberhadseregének a megalapítása és talán működésének csúcspontja is, ami két akkori vezetője szaktudásának és kompetenciájának volt köszönhető, amelyek révén feltehetően komolyabb kibertámadásokat is elkövethettek. Jelentőségükre abból lehet következtetni, hogy pár hónap eltéréssel mindkettőjükkel dróntámadás keretében végzett Rakkában az amerikai hadsereg.[33]

A 2017-es jelentésben[34] a korábbinál kiemeltebben kezelik a kibertér irányából érkező fenyegetések jelentőségét, mivel a támadások rombolják a globális és kormányzati intézményekbe, normákba vetett bizalmat, és emellett még gazdasági károkat is okoznak. Egyre komolyabb kockázatot jelentenek a kiberfenyegetések a kritikus infrastruktúrákra, a biztonságra és a gazdasági fejlődésre. Emellett láthatók a pszichológiai hatások, következmények is. A terrorista csoportok továbbra is elsősorban toborzásra, szervezkedésre-koordinációra, pénzügyi források előteremtésére és propaganda terjesztésére használják az online teret. Emellett az ISIS keresni fogja a lehetőséget arra is, hogy szenzitív információkat szerezzen meg és szivárogtasson ki amerikai állampolgárokról ahhoz hasonlóan, ahogy az 2015-ben is történt az amerikai hadsereg állománya esetében. Az ukrán áramhálózat megtámadása kapcsán hívják fel a figyelmet arra, hogy a kibertérből indított, kritikus infrastruktúrákat érintő támadásoknak a fizikai térben is lehetnek következményei, okozhatnak kárt. Külön tesznek említést a kibertámadások gazdasági és biztonsági következményeiről. Ez utóbbi esetében az amerikai védelmi szektort érő folyamatos ipari kémkedési törekvésekre és az üzleti hírszerzés veszélyeire mutatnak rá, majd

31 Director of National Intelligence 2016.

32 A dolgok internete, mesterséges intelligencia, virtuális/kiterjesztett valóság, külföldi országok által amerikai adatokon végzett adatbányászati tevékenység jelentette kockázatokat és sérülékenységeket emelték ki.

33 Az egyik Briton Junaid Husszein (Abu Husszein al-Britani, TeaMpoisoN) volt, aki 2013-ban utazott Szíriába, és csatlakozott az IS-hez, miután fél évet ült egy brit börtönben Tony Blair személyes adatainak ellopása és nyilvánossá tétele miatt. Britont 2015 augusztusában Rakkában lőtték le (Ackermann 2015). A másik említésre méltó hacker a szintén brit kötődéssel rendelkező Siful Haque Sujan volt, aki Briton utódja volt, és 2015 decemberében vesztette életét egy célzott dróntámadás következtében (*IS computer hacker Siful Haque Sujan killed in air strike* 2015).

34 Director of National Intelligence 2017.

ezt követően szintén különálló alfejezetet szenteltek a kibertámadások pszichológiai hatásainak is. A 2018. évi elemzés[35] a terrorszervezetek kapcsán megismételte az előző évi értékelést, a módszerek tekintetében megemlítésre került a weboldal defacement és a túlterheléses (DDoS-) támadás a gyengén védett hálózatok ellen. A kiberbűnözés kapcsán megjegyzik, hogy még jobban kezd elmosódni a határ a bűnözői és az állami tevékenység között.

A 2019-es jelentés[36] szerint a terroristák a kiberműveletek révén kompromittáló vagy személyazonosításra alkalmas információkat szerezhetnek meg és hozhatnak nyilvánosságra, és ezeket az adatokat felhasználhatják kényszerítésre, zsarolásra, vagy arra, hogy áldozataik ellen fizikai támadásokat kezdeményezzenek és tegyenek lehetővé. A terrorista csoportok figyelmeztetés nélkül is okozhatnak bizonyos zavaró hatásokat – weboldalakat rongálhatnak meg, vagy szolgáltatásmegtagadási támadásokat hajthatnak végre a rosszul védett hálózatok ellen. A nyilvánosan és kereskedelmi forgalomban egyre nagyobb mennyiségben hozzáférhetővé váló kibereszközök következtében folyamatosan növekszik az attribútum nélküli támadások száma, ezáltal megnő a téves felelősségre vonás és a téves válaszlépések kockázata. A következő évben nem készült jelentés, viszont a korábbiak esetében fontosnak tartom megjegyezni, hogy a hagyományos értelemben vett terrorizmus már csak a negyedik helyen szerepelt, jelentősége fokozatosan csökkent, miközben a kibertér egyre szélesebb palettáját szolgáltatja a fenyegetéseknek.

A 2021-es évtől[37] teljesen új struktúrában készítik az elemzést, aminek eredményeként elsőként a legnagyobb kockázatot jelentő országokat (Kína, Oroszország, Irán, Észak-Korea), illetve az általuk jelentett fenyegetések teljes spektrumát ismertetik, majd ezt követően térnek rá a regionális fenyegetésekre. A kibertérrel foglalkozó fejezetben a terrorszervezetek már egyáltalán nem szerepelnek, alapvetően az állami, illetve államok által szponzorált és a szervezett bűnözői csoportok jelentette fokozott kockázatokat taglalja csak. A 2022-ben készült jelentés[38] a terrorista csoportokra már csak a transznacionális kérdésekről, fenyegetésekről szóló fejezeten belül tér ki, miközben a kibertérben folytatott tevékenységükről már említést sem tesz. A legutoljára, 2023 februárjában kiadott amerikai hírszerző közösség által készített elemzésben[39] új fejezetként jelenik meg, hogy az autoriter rezsimek – általában – hogyan használják fel a digitális technológiákat az elnyomás, megfélemlítés, megfigyelés erősítésére, a szabadságjogok korlátozására és a rosszindulatú befolyásolásra.

35 Director of National Intelligence 2018.
36 Office of the Director of National Intelligence 2019.
37 Office of the Director of National Intelligence 2021.
38 Office of the Director of National Intelligence 2022.
39 Office of the Director of National Intelligence 2023.

Az egyéb transznacionális kérdések között találhatók meg a diszruptív technológiák jelentette kockázatok, a digitális technológia elnyomó rezsimek általi felhasználása, proliferáció, migráció, transznacionális szervezett bűnözői csoportok és végül a globális terrorizmus. A terrorizmus kapcsán a kiber aspektus 2023-ban sem jelenik meg, sőt a terjedelmet nézve is jelentős csökkenés látható a korábbi évekhez képest.[40]

Az elmúlt tizenhét év amerikai hírszerzési jelentéseinek áttekintése alapján látható, hogy a hagyományos és a kiberterrorizmus mint kockázat visszaszorulóban van. Helyét, helyüket – a békeidő ellenére – a nemzetállamok vették át, és velük párhuzamosan egyre nagyobb fenyegetést jelentő tényezővé váltak a transznacionális szervezett bűnözői csoportok is, amelyeknek a tevékenységi köre, terepe szintén kiegészült a kibertérrel. A több mint másfél évtizednyi elemzés áttekintése révén az is láthatóvá vált, hogy az online befolyásolási, ellenérdekelt támadótevékenységeknek, illetve ezek társadalomra gyakorolt pszichológiai hatásának nemzetbiztonsági vetületei is lehetnek.

A KIBERTERRORIZMUS PSZICHOLÓGIÁJA

A 21. században a kibertérben tapasztalható agresszió mindennapossá vált, a legtöbb ember számára azonban még mindig csak a pénzügyi információkat vagy más személyes adatokat célba vevő kiberbűnözők formájában jelent valóságot, vagy ölt formát. Politikai indíttatású támadások is fenyegethetik őket, de ezek inkább a kormányokat és a vállalatokat érintik, mint az átlagpolgárokat, de természetesen ez utóbbira is lenne példa. Az átlagember számára valószínűleg sokkal ijesztőbbnek tűnik egy plázában lövöldöző vagy egy repülőtéren robbantó terrorista gondolata, mint például az észtországi kormányzati hálózatokat megzavaró orosz hackerek[41] vagy egy amerikai élelmiszeripari cég, a JBS S. A. megtámadása zsarolóvírussal, aminek következtében leállt a vállalat működése.[42]

Az emberek szinte naponta szembesülnek a kibertérben agresszióval. A hackerek adatokat lopnak el, törölnek ki vagy kérnek váltságdíjat érte, banki ügyfelektől csalnak ki bankkártyaadatokat, majd elveszik a pénzüket, személyazonosságot lopnak,

[40] Érdemes megjegyezni, hogy az elmúlt pár évben a terrorizmussal párhuzamosan a jelentésekbe bekerültek a szélsőjobboldali extremizmus és idegengyűlölet által generált bűncselekmények, fegyveres támadások, amelyek egyre komolyabb – elsősorban – közbiztonsági kockázatot jelentenek.

[41] Council on Foreign Relations 2007.

[42] Egyik támadást sem terrorszervezet követte el, hanem orosz hátterű hackercsoportok. *JBS: FBI says Russia-linked group hacked meat supplier* 2021.

vagy rosszindulatú vírusokat telepítenek. Sok esetben a hackerek egyszerű anyagi haszonszerzésre törekvő bűnözők, néha azonban politikai indítékaik is vannak. Vannak hacktivisták vagy kiberaktivista csoportok, mint az Anonymous, vannak terrorcsoportok, mint a Hamász vagy az Iszlám Állam, és természetesen léteznek a nemzetállamok, mint Észak-Korea, Irán, Kína vagy Oroszország által anyagilag támogatott csoportok, amelyeket általában nem a pénz motivál, hanem politikai célokat követnek, hogy társadalmi változásokat gerjesszenek, politikai előnyt szerezzenek, vagy megbénítsák az egyik ellenséget. Néha békés, máskor viszont erőszakos eszközökkel lépnek fel. Ugyanakkor nyílt forrású információk alapján nem keletkeztek arra vonatkozó ismeretek, hogy kiberterroristák valamilyen kibertérben végrehajtott akció révén megöltek vagy megsebesítettek volna bárkit is. Az ezzel való fenyegetésre természetesen számos példa található, főleg az ISIS online propagandaanyagaiban. Végső soron a terrorizmus célja nemcsak a fizikai pusztítás, hanem a pszichológiai hatás, a félelem keltése minél szélesebb körben. Michael L. Gross és munkatársai[43] a kutatásaik során arra jutottak, hogy a kiberagresszió, a kiberterrorizmus pszichológiai hatásai ugyanolyan erősek lehetnek, mint a valódi, fizikai térben megvalósuló támadásoké.[44] Az emberi biztonság, biztonságérzet ugyanis a legalapvetőbb szinten azt jelenti, hogy képesnek kell lenniük arra, hogy indokolatlan félelemtől, szorongástól és rettegéstől mentesen éljenek. A hagyományos terrorizmus súlyosbítja a bizonytalanság érzését és a fenyegetettség érzékelését. Kérdés, hogy vajon a kiberterrorizmus is hasonló hatásokat okoz-e? A kiberterrorizmusnak sok arca van, ahogy a tömegek pszichológiájának is. Kutatásaik eredményeként Grossék bemutatták, hogy még a kiberterrorizmus nem halálos, banálisnak tűnő formái is jelentős hatással vannak az áldozattá vált lakosság hozzáállására. Kísérleteik során arra jutottak, hogy létezik „kiberterrorizmus-hatás", amely azt jelenti, hogy a terroristák az online téren keresztül is elérhetik, hogy a kinetikus terrorizmushoz hasonló félelmeket keltsenek. Ilyenformán a kiberterrorizmus jóval túlmutat a kiberbűnözésen, még akkor is, ha módszerei – személyazonosság-lopás, adatok megsemmisítése és a szolgáltatások megzavarása – néha hasonlóak. Nemcsak a félelemkeltés tekintetében van eltérés a kiberbűnözés és a kiberterrorizmus között. Egy későbbi kutatás során Gross és munkatársai[45] ugyanis megfigyelték a lakosság militarizálódását, vagy legalábbis az erre való fokozottabb hajlandóságot egy-egy támadást követően, és hasonlóan a fizikai térben megvalósuló terrorizmushoz, az állammal és az általa nyújtott biztonsággal szembeni elvárások is hasonló, növekvő tendenciát mutattak.

[43] Gross–Canetti–Vashdi 2016.

[44] Ma már az emberek többsége sem kételkedik abban, hogy az online propagandaanyagok szerepet játszhatnak az egyes emberek radikalizációjában.

[45] Shandler et al. 2022.

Az amerikai, brit és izraeli állampolgárok körében elvégzett kutatás során megfigyelték azt is, hogy kizárólag egy halálos kimenetelű kibertámadás generálna olyan érzelmeket a társadalmon belül, amely militarizálódásba, illetve katonai ellencsapás követelésévé alakulhat át. A kutatás arra is rávilágított, hogy önmagában a terrorral fenyegetés nem alakít ki ilyen jellegű érzelmeket, kizárólag a düh.

ÖSSZEGZÉS

Az internettől és a technológiától való függőségünk megköveteli, hogy feltegyünk magunknak egy kérdést: milyen hatással lenne az életünkre, ha a minket körülvevő technológiák működése leállna? Sokan nincsenek tisztában az elmúlt két évtizedben lezajlott információs forradalom valódi kiterjedtségével és mélységével. Amikor a technológiától való személyes függőségünkre gondolunk, általában a Facebook-fiókunkhoz való hozzáférés, az e-mailek és esetleg az online banki szolgáltatások jutnak eszünkbe. Gyakran figyelmen kívül hagyjuk, hogy a társadalom és a kormányzat alapvető funkciói mennyire függenek ugyanezektől a technológiáktól. Ilyen például a tömegközlekedés, vagy az áram termelése és szolgáltatása. Az alapvető, létfontosságú infrastruktúrák működésének kártékony és szándékos megzavarásának kockázata valós, és az elmúlt több mint két évtized – nyílt forrásból elérhető információkra alapozott – tapasztalatait figyelembe véve úgy tűnik, hogy a kiberterroristák jelentették rá a legminimálisabb veszélyt. Helyüket a nemzetállamok kiberhadseregei vagy az általuk szponzorált hackercsoportok, illetve kiberbűnözők töltötték be. A mai napig tehát a kiberterroristák nem öltek meg és nem sebesítettek meg senkit, és nem pusztítottak el sikeresen egyetlen kritikus infrastruktúrát sem. Hogy ez a terroristák támadói kompetenciái hiányának vagy az Egyesült Államok és szövetségesei védelmi képességeinek, vagy a szerencsének köszönhető-e, azt nehéz megállapítani. Úgy tűnik tehát, hogy jelenleg a kiberterrorizmus – Denning által lehatárolt típusa – nem jelent közvetlen fenyegetést, azonban a kockázatértékelési mátrixban mindig szerepeltetni kell ezt az attribúciót is.[46]

Ebben feltehetően szerepet játszik, hogy a megtámadni kívánt rendszerek rendkívül összetettek, ezért a támadást nehezebb lehet irányítani és elérni a kívánt mértékű kárt, hatást. Ráadásul amennyiben nem sérülnek meg emberek, a hatáskeltés szempontjából is kisebb vonzerővel bír a kibertér használata. A valószínűsíthető okok között lehet említést tenni még arról a tényezőről is, hogy a terroristák nem

[46] Kiberbiztonsági szempontból nagy valószínűséggel nem kíván meg más jellegű felkészülést a kiberhadviseléshez vagy kiberbűnözéshez képest.

szívesen próbálnak ki új módszereket, hacsak nem látják a régieket alkalmatlannak, különösen akkor, ha az új módszerek hatékony alkalmazásához jelentős tudásra és készségekre van szükség. A terroristák általában ragaszkodnak a már kipróbált és jól bevált módszerekhez, a támadás újdonsága és kifinomultsága sokkal kevésbé fontos szempont. Ennek tudható be, hogy aktuálisan is egy autóba rejtett robbanóanyag vagy egy teherautó felhasználása tömegbe hajtásra sokkal nagyobb fenyegetést jelent, mint egy logikai bomba, amelyet kritikus információs infrastruktúrákkal szemben vetnek be.

A terroristák következő generációi már ebben a digitális világban nőnek fel, aminek az eredményeként drasztikus változás volt tapasztalható már az ISIS működése során is abban, ahogy a különböző közösségimédia-felületeket használták az évek előrehaladtával egyre professzionálisabb módon. A célzott, egyértelműen romboló indítékú kiber-fizikai támadásokig azonban még nem jutottak el. Az új digitális generáció talán majd nagyobb potenciált lát a kiberterrorizmusban, mint a kétezres évek első két évtizedének terroristái, és ebből adódóan a hackeléssel kapcsolatos tudásuk és képességeik szintje is magasabb lesz.

A kiberterrorizmus elleni háború folytatásával azonban egyre világosabbá válik, hogy a nemzeti érdekek védelme csak a kihívás, fenyegetés egyik fele, terepe. A kiberhadviselés elleni fellépés során gyakran elvész az emberi dimenzió szerepe. Miközben a tudósok és a politikai döntéshozók aggodalmukat fejezik ki a kiberterrorizmus nemzetbiztonsági veszélyeivel kapcsolatban, kevés információ, kutatás áll rendelkezésre az emberi – pszichológiai – biztonságra gyakorolt hatásairól, pedig a jelentősége megkérdőjelezhetetlen.

FELHASZNÁLT IRODALOM

Ackerman, Spencer (2015): Junaid Hussain: British Hacker for ISIS Believed Killed in US Air Strike. *The Guardian,* 2015. augusztus 27. Online: https://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike

Blake, Andrew (2016): Ardit Ferizi, hacker who aided Islamic State, sentenced for helping terror group with kill list. *Washington Times,* 2016. szeptember 24. Online: https://www.washingtontimes.com/news/2016/sep/24/ardit-ferizi-hacker-who-aided-islamic-state-senten/

Brenner, Susan W. (2006): Cybercrime, cyberterrorism and cyberwarfare. *Revue Internationale de Droit Pénal,* 77(3–4), 453–471. Online: https://doi.org/10.3917/ridp.773.0453

Denning, Dorothy E. (2001): *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.* Online: http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf

Global ransomware attack causes turmoil. *BBC,* 2017. június 28. Online: https://www.bbc.com/news/technology-40416611

Gross, Michael L. – Canetti, Daphne – Vashdi, Dana R. (2016): The psychological effects of cyber terrorism. *The Bulletin of the Atomic Scientists,* 72(5), 284–291. Online: https://doi.org/10.1080/00963402.2016.1216502

IS computer hacker Siful Haque Sujan killed in air strike. *BBC,* 2015. december 31. Online: https://www.bbc.com/news/uk-wales-35206038)

Jammu and Kashmir Police cracking down on white-collar jihadis. *The Tribune,* 2021. augusztus 30. Online: https://www.tribuneindia.com/news/j-k/jammu-and-kashmir-police-cracking-down-on-white-collar-jihadis-303976

JBS: FBI says Russia-linked group hacked meat supplier. *BBC,* 2021. június 3. Online: https://www.bbc.com/news/world-us-canada-57338896

Nelson, Bill et al. (1999): *Cyberterror: Prospects and Implications.* Monterey: Center for the Study of Terrorism and Irregular Warfare. Online: https://apps.dtic.mil/sti/pdfs/ADA393147.pdf

Plotnek, Jordan J. – Slay, Jill (2021): Cyber terrorism: A homogenized taxonomy definition. *Computers and Security,* 102(2), 102145. Online: https://doi.org/10.1016/j.cose.2020.102145

Shamah, David (2012): Latest viruses could mean end of world as we know it, says man who discovered Flame. *The Times of Israel,* 2012. június 6. Online: https://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/

Shandler, Ryan et al. (2022): Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment. *British Journal of Political Science,* 52(2), 850–868. Online: https://doi.org/10.1017/S0007123420000812

Wilson, Clay (2008): *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* RL32114. Congressional Research Service. Online: https://www.everycrsreport.com/reports/RL32114.html#_Toc216519385

Egyéb források

Council on Foreign Relations (2007): *Estonian Denial of Service Attack.* Online: https://www.cfr.org/cyber-operations/estonian-denial-service-incident

Director of National Intelligence (DNI) (2006): *Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence.* Online: https://www.dni.gov/files/documents/Newsroom/Testimonies/20060202_testimony.pdf

Director of National Intelligence (DNI) (2007): *Annual Threat Assessment of the Director of National Intelligence.* Online: https://www.dni.gov/files/documents/Newsroom/Testimonies/20070111_testimony.pdf

Director of National Intelligence (DNI) (2008): *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee.* Online: https://www.dni.gov/files/documents/Newsroom/Testimonies/20080227_testimony.pdf

Director of National Intelligence (DNI) (2009): *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee.* Online: https://www.dni.gov/files/documents/Newsroom/Testimonies/20090310_testimony.pdf

Director of National Intelligence (DNI) (2010): *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence.* Online: https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf

Director of National Intelligence (DNI) (2013): *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence.* Online: https://www.dni.gov/files/NCTC/documents/news_documents/2013_03_12_SSCI_Worldwide_Threat_Assessment.pdf

Director of National Intelligence (DNI) (2014): *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence.* Online: https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

Director of National Intelligence (DNI) (2015): *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee.* Online: https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Director of National Intelligence (DNI) (2016): *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee.* Online: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Director of National Intelligence (DNI) (2017): *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*. Online: https://www.dni.gov/files/documents/Newsroom/Testimonies/SASC%202017%20ATA%20SFR%20-%20FINAL.PDF

Director of National Intelligence (DNI) (2018): *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*. Online: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Office of the Director of National Intelligence (ODNI) (2019): *Statement For The Record Worldwide Threat Assessment of the US Intelligence Community.* Online: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Office of the Director of National Intelligence (ODNI) (2021): *Annual Threat Assessment of the U. S. Intelligence Community.* Online: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Office of the Director of National Intelligence (ODNI) (2022): *Annual Threat Assessment of the U. S. Intelligence Community.* Online: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

Office of the Director of National Intelligence (ODNI) (2023): *Annual Threat Assessment of the U. S. Intelligence Community.* Online: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf