Forró Tamás

KIBERTERRORIZMUS: MIT HOZ A JÖVŐ?

„Aki a jövőről fogalmaz meg állításokat, az csal vagy hazudik."[1] Hogy Csányi Vilmos Széchenyi-díjas biológus, akadémikus valóban jogosnak tűnő gondolatait ismerve miért is bocsátkozok valamiféle jóslásba, annak igen prózai okai vannak. A meglévő, sajnos közel sem korlátlan erőforrásainkat – véleményem szerint – akkor tudjuk minél hatékonyabban felhasználni, ha tisztában vagyunk a saját képességeinkkel, és a lehető legjobban megpróbáljuk feltárni a jövőbeli fenyegetéseket. E rövid szerzemény célja is pontosan ez kíván lenni a kiberterrorizmus kapcsán, azaz hogy a terület múltjának, jelenének rövid áttekintésével választ kapjunk arra a kérdésünkre, hogy valós fenyegetés-e a kiberterrorizmus, avagy mit hoz a jövő.

Az emberiség történetében az idő előrehaladtával – a technikai vívmányoknak köszönhetően – folyamatosan nyíltak meg a hadviselés új színterei. Miközben megtanultuk kezelni vagy legalább elfogadni a szárazföldön, vízen, levegőben és az űrben jelen lévő fenyegetéseket, megjelent egy új, nehezebben megfogható rész, a kibertér, amelyet a NATO[2] 2016-ban ismert el az ötödik katonai műveleti területnek.[3] A kibertér, az internet világa forradalmian új lehetőségeket nyitott meg az élet minden területén. Lehetővé vált, hogy az otthonunk kényelméből érjük el a munkahelyi hálózatunkat és az ott kezelt információkat, hogy a világ bármely pontjáról ránézzünk a nappalinkba telepített webkamera képére, hogy a hűtésünket, fűtésünket távolról szabályozzuk, vagy akár az is, hogy a termelési folyamatokat bárhonnan nyomon követhessük, és szükség esetén be is avatkozhassunk abba a hálózaton elérhető millió és millió érzékelőn, vezérlőn keresztül.

Ugyanakkor abban a pillanatban, amikor ez számunkra elérhetővé vált, potenciálisan ugyanúgy vált elérhetővé az internetet használó további több mint ötmilliárd felhasználó[4] számára is. Természetesen nem feltétlenül olyan egyszerűen, mint nekünk (például infrastrukturális adottságok miatt), de nem is biztos, hogy lényegesen nehezebben. Az a tény, hogy ilyen számosságú és értékű rendszer és információ

1 Nagy 2017.
2 Észak-atlanti Szerződés Szervezete (angolul: North Atlantic Treaty Organisation).
3 NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit.
4 Internet Usage Statistics [é. n.].

DOI: https://doi.org/10.36250/01259_18

ilyen könnyedén elérhető, értelemszerűen felkeltette a figyelmét több csoportnak is. Az unatkozó fiataloknak, akik a (kétes) hírnévért, vagy pusztán az izgalom miatt törnek fel rendszereket, a bűnözőknek, akik például az adataink, információink ellopásával, elérhetetlenné tételével kívánnak pénzt szerezni, a hacktivistáknak, akik valamilyen politikai vagy társadalmi eszmét óhajtanak kikényszeríteni, vagy legalább közzétenni, és természetesen a terroristáknak is, akik lényegében az összes fenti tevékenységben érdekeltek valamilyen módon.

ELŐZMÉNYEK, A MÚLT

A történelemben számos példát láthattunk arra, hogy egy elsősorban hadászati célokra fejlesztett eszköz, technológia kisebb-nagyobb módosítások után a civil életben is feltűnik. Ez a tendencia a 21. század elejére azonban – elsősorban az információ-technológiának köszönhetően – megfordulni látszik. Az ezen a területen megjelenő, a korábbi időszakokhoz képest lényegesen rövidebb életciklusú innovációk és fejlesztések debütálnak később katonai alkalmazásban. A kibertér megjelenése és rendkívüli ütemű bővülése csak katalizálta ezt a folyamatot, egy ritkán látott mértékű változást hozva ezzel a hadviselésben. A támadó és az általa alkalmazott módszer „láthatatlanná válásával", a fizikai határok eltűnésével ez valóban új dimenziót jelent. Értelemszerűen a terrorizmus sem „engedhette meg magának", hogy kimaradjon ebből a folyamatból, hiszen ezzel lényegesen ideálisabbak lettek a terrorcselekmények elkövetésének feltételei, illetve az internetet használó több milliárd felhasználó eléréséről is lemondana.

A kiberterrorizmus mint kifejezés már 1979-ben megtalálható volt egy svéd számítógépes bűnözésről szóló jelentésben, ugyanakkor a büntetőjog-irodalomban széles körben csak a 2001. szeptember 11-ei terrortámadásokat követően terjedt el.

> „Érdemes megjegyezni, hogy politikai célú támadásokat már ezt megelőzően is indítottak az interneten keresztül, így például az 1999-es koszovói konfliktus során. A Jugoszláviát ért bombázásokat követően túlterheléses, ún. DDoS-támadások (Distributed Denial of Service)[5] indultak a NATO weboldalaival szemben, és jugoszláv honlapok működését is megpróbálták ellehetetleníteni vagy tartalmukat módosítani. A NATO szándékosan nem pusztította el az ország internetelérést biztosító fizikai infrastruktúráját, abban bízva, hogy az interneten keresztül szerzett információk a jugoszláv kormány ellen fordíthatják a lakosságot."[6]

[5] Magyarul: Elosztott szolgáltatásmegtagadással járó támadás.

[6] Dornfeld 2019.

Fontos megjegyezni, hogy ezek a tevékenységek definíció alapján nem feltétlenül felelnek meg a kiberterrorizmus minden szükséges jegyének. A fenti eseményeknek és az informatika elterjedésének köszönhetően már az 1990-es években elkezdtek napvilágot látni azok a gondolatok, miszerint a „holnap terroristája" több kárt tud okozni a számítógép billentyűzete segítségével, mint egy bombával.[7] A 2001. szeptember 11-ei terrortámadásokat követően gondolati szinten történt azonban egy ugrásszerű növekedés. Ennek oka a félelemben, vagy akár mondhatjuk, hogy sokkban lévő társadalom szempontjából érthető volt, hiszen további rémálomszerű támadásokra lehetett számítani. A fizikai biztonsági intézkedések jelentős szigorítása, az informatikához társított misztikum, illetve elterjedésének gyorsasága valóban logikusan eredményezhette volna azt, hogy a következő – a Világkereskedelmi Központ[8] ikertornyainak ledöntéséhez mérhető – támadás a kibertérben fog bekövetkezni, elsősorban a kritikus (információs) infrastruktúrát célozva.

A kiberterrorizmussal kapcsolatos félelmek gyökerei az 1990-es évek végére, a 2000-es évek elejére vezethetők vissza. Az internet, az informatikai és gyakorlatilag az információs társadalom lehetőségeinek minden korábbi elképzelést túlszárnyaló fejlődésével egyre több felelős döntéshozó számára vált nyilvánvalóvá, hogy egy modern állam és annak szinte minden szervezete milyen jelentős mértékben is függ a digitális technológiáktól. Ebből fakadóan a kiberterorrizmus által jelentett veszély felkeltette a vezetők, politikusok figyelmét is. A 2001. szeptember 11-ei terrortámadások után a pszichológiai, politikai és gazdasági tényezők még inkább felerősítették ezeket a félelmeket. Lényegében az akkori kor két legmeghatározóbb félelme egyesült a kiberterrorizmusban: a véletlenszerű áldozattá válás jól keveredett a számítógépes technológiával kapcsolatos bizalmatlansággal.

Ezek a félelmek ugyanakkor nem voltak teljesen alaptalanok. Több olyan eset is történt, amelyben egy kevésbé képzett aktor követett el olyan tevékenységet a kibertérben, amely a fizikai térben történő valós károkozással vagy akár sérüléssel is járt. Ezek alapján valóban jogosnak tűnhetett az a félelem, miszerint ha egy tinédzser egyedül képes ilyen jellegű akcióra,[9] akkor mire lehet képes egy felkészült, elszánt, jelentős erőforrások felett diszponáló terrorista csoport.

Az új technológiai lehetőségeket azonban elsősorban más célból kezdték használni a terroristák. A legkönnyebben megvalósítható eszközként honlapokat, internetes fórumokat hoztak létre abból a célból, hogy aktívan kommunikálják motivációjukat, céljaikat, megszólítsák a társadalmat, illetve ezzel passzív módon elérhették azt is,

[7] „Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." National Research Council System Security Study Committee 1991.

[8] Angolul: World Trade Center (WTC).

[9] Squatriglia 2008.

hogy ezeken a platformokon beszéljenek róluk, tetteikről. „A hadviselés, illetve a terrorizmus módszereire, napjainkban kialakult és várhatóan a jövőben kialakuló formáira nagy hatást gyakorol a média, illetve az a körülmény, hogy a technikai fejlődés révén a hírek egyre hamarabb, szinte már valós időben, egyre nagyobb tömegeket érnek el, így szállítva a terroristák üzeneteit az információs társadalom tagjaihoz. A terroristák »csapdát« állítanak a média számára, és amikor az ráveti magát az elé helyezett történetre, azt kell észrevennie, hogy idegen üzenet került a rendszerbe. A terroristák taktikája lényegében kivédhetetlen, mivel a szabad médiában piaci verseny uralkodik, és a médiaipar egyik szereplője sem engedheti meg magának, hogy ne vegyen tudomást a terroristák által rendezett drámákról. Így olyan témák kerülnek reflektorfénybe, melyek korábban nem léteztek a média »valóságában«, illetve a hivatalos politika részéről száműzve voltak onnan."[10] A rendelkezésre álló információk alapján a terroristák tevékenysége elsősorban erre a területre terjed ki, valamint új tagok toborzására, biztonságos kommunikációra, terroristák kiképzésével kapcsolatos kiadványok közzétételére, működésük finanszírozására, egyéb erőforrások, képességek gyűjtésére, szolgáltatások igénybevételére, valamint a lehetséges célpontokról történő információgyűjtésre használják a kiberteret.

A JELEN

A kiberterrorizmus jelenének feltérképezésére a közelmúltban történt büntetőjogi eseteket és az ISIS „hackerének" történetét hívtam segítségül, amelyeken át képet kaphatunk az elkövetés jellegéről, módjáról.

Az Amerikai Egyesült Államokban 2016-ban emeltek először vádat kiberterrorizmus miatt. Az eljárás során az Ardit Ferizi nevű hackert vádolták azzal, hogy állítólag feltört egy katonai honlapot, és ellopta a kormányzati és katonai személyzet neveit, címeit és egyéb személyes adatait, majd eladta azokat az ISIS-nek.[11] (Islamic State of Iraq and Syria – Iraki és Szíriai Iszlám Állam).[12] A fenti tényállás áttekintése után azonban joggal hiányolhatjuk a „klasszikus" terrorizmus definiálása során megállapított kötelező elemek jelentős részét.

Lényegesen jelentősebb fejlődési lépcsőfoka és szereplője volt azonban a kiberterrorizmusnak a brit származású Junaid Husszein, aki egészen a 2015 augusztusában, amerikai dróntámadásban bekövetkezett haláláig az Iszlám Állam hackere és egyben

[10] Papp 2018.
[11] Blake 2016.
[12] Blake 2016.

a legtermékenyebb angol nyelvű közösségimédia-propagandistája volt.[13] Pakisztáni szülők gyermekeként az angliai Birminghamben élt. Az ismerősei a való életben egy csendes, visszahúzódó gyermekként számoltak be róla, aki csak a számára is érdekes, fontos témákról beszélt szenvedélyesen. Kortársaihoz hasonlóan ő is sok időt töltött a számítógép előtt ülve, online játékokkal játszva. Az itteni barátai alapján azonban egy igen érdekes kép rajzolódott ki róla, ugyanis személyisége és viselkedése totális ellentéte volt annak, amit a való életben mutatott magáról. „Száz százalékban nyitott, extrovertált, vicces, szellemes. De legfőképpen rendkívül gondoskodó és együttérző" – mondta az egyik ilyen hacktivista. Élete 11 éves korában vett gyökeres fordulatot, amikor egy, a kibertérben ért sérelme miatt elkezdett a hackeléssel foglalkozni. Elmondása szerint csatlakozott néhány online hackerfórumhoz, oktatóanyagokat, fórumokat olvasott, és ettől kezdve foglalkozott webhelyek, szerverek feltörésével azért, hogy bosszút állhasson.[14] Képességeinek fejlődésével egyidejűleg a politikai aktivizmus felé fordult.

Bár Husszein egyértelműen rajongott a muszlim társadalmak történelméért, nem érdeklődött különösebben az iszlám iránt. Miközben a neten kutatott a muszlim kérdéskörrel kapcsolatban, elkezdte feltörni a weboldalakat abból a célból, hogy felhívja a figyelmet a problémákra szerte a világon. Husszein e tevékenységével nem volt egyedül. Maga köré gyűjtött egy csoport hacktivistát, akik közül sok hasonló politikai beállítottságú volt, de nem voltak feltétlenül azonos etnikumúak. Tizenöt évesen hozta létre saját fórumát (a poison.org-ot), majd később ebből alakult ki a TeaMpoisoN, ahol TriCk álnéven vált ismertté. Ebben az időszakban törték fel a volt brit miniszterelnök, Tony Blair egyik belső munkatársának e-mail-fiókját,[15] ami után Husszein számos kormánytisztviselővel kapcsolatos bizalmas anyagot osztott meg az interneten, és ez azonnal híressé tette. A TeaMpoisoN másik nagy nyilvánosságot kapott támadása 2012 áprilisában történt, amikor telefonos szolgáltatásmegtagadási (DoS[16]) támadást indított az Egyesült Királyság Terrorelhárítási Parancsnokságának forródrótja ellen. A támadás következtében az iroda telefonvonalait bombázta egy robothang, amely a „Team Poison" kifejezést ismételte. E cselekmények után a hatóságok letartóztatták. A börtön a jelek szerint vízválasztó időszak volt számára. Bebörtönzése előtt Husszein alapvetően inkább „szélsőségesnek" titulálta magát, és úgy tűnt, hogy a muszlimokkal szembeni vélt vagy valós igazságtalanságok ellen harcol, de a politikai nézeteit inkább az anarchizmushoz hasonlónak minősítette.

[13] Hamid 2018.

[14] Kovacs 2012.

[15] Roberts 2012.

[16] Denial-of-Service attack (DoS attack), magyarul: szolgáltatásmegtagadással járó támadás vagy túlterheléses támadás.

A rövid büntetése alatt azonban a börtönben vélhetően radikalizálódott. Szabadulása után nem sokkal, 2013-ban hagyta el Angliát, és csatlakozott az ISIS-hoz,[17] ahol elsősorban propagandista és toborzó szerepet töltött be. Noha Husszeint az Islamic State Hacking Division (ISHD – Iszlám Állam Hacker Divízió) vezetőjének tartották, jelenleg nem tisztázott, hogy személyesen végzett-e ilyen tevékenységet Szíriában. Amennyiben végzett is, az lényegesen kisebb léptékű volt a toborzási és kiberterror-koordinációs tevékenységénél. Ő szervezte be ugyanis a korábban már említett Ardit Ferizit, és ugyancsak ő volt a felbujtója számos hozzá forduló személynek. Ezek közül az egyik példa Munir Abdulkader ohiói főiskolai hallgató esete, aki 2015 tavaszán kereste meg Husszeint. Miután lebeszélte Abdulkadert arról, hogy Szíriába jöjjön, Husszein utasította, hogy rabolja el az amerikai hadsereg egyik tagját, és vegye videóra meggyilkolását, illetve hogy támadjon egy rendőrőrsre Cincinnati közelében.

Bár Abdulkadert letartóztatták, és 20 év börtönre ítélték,[18] mielőtt ezeket végrehajthatta volna, mégis komoly jelzés volt a hatóságok számára ez az új irány. Korábban nem igazán volt példa arra, hogy a leendő újoncokat arra ösztönözték, hogy maradjanak lakóhelyükön (jellemzően az Egyesült Államokban vagy Európában), és ott hajtsanak végre támadásokat. A toborzók így szinte lehetetlenné tették a hatóságok számára, hogy észlelhessék azokat a tipikus viselkedéseket és jeleket (például a gyanús utazásokat, pénzmozgásokat stb.), amelyek korábban előre jelezhették a támadás tényét. További óriási előny volt a terrorcsoportok számára, hogy ez a tevékenységük elenyésző költséggel járt, egyáltalán nem jelentett komoly veszteséget (hálózat és „modus operandi" kompromittálódása, befektetett eszközök, kapcsolatok elvesztése), ha a potenciális elkövető esetleg lebukik, és a terrorcselekmény elkövetése meghiúsul. Husszein alapvetően egy olyan fenyegetést képviselt, amelynek megjelenésétől 2001 óta féltek a hatóságok; egy, a technológiához értő terroristát, aki a modern digitális élet eszközeit használja arra, hogy egy terrorista csoport hatókörét messze kiterjessze a fizikai helyén túlra. 2015 nyarán sikeresen végrehajtotta az egyik „legglobálisabb" terrorista műveletet, amelyet valaha láttunk: egy pakisztáni származású, Szíriában élő, brit terrorista beszervezett egy koszovói hackert, aki számítástechnikát tanult Malajziában, hogy lehetővé tegye az amerikai katonák elleni támadást az Egyesült Államokban.

Életútjának rövid bemutatását azért is tartottam kiemelten fontosnak, mert az általa koordinált és folytatott tevékenység már sokkal inkább beleillik abba, amit az átlagos állampolgár kiberterrorizmus alatt ért. Véleményem szerint a jövőben is ez lehet az egyik jellemző megjelenési formája a kiberterrorizmusnak.

[17] Iraki és Szíriai Iszlám Állam (angolul: Islamic State of Iraq and Syria).

[18] Office of Public Affairs U.S. Department of Justice 2016.

MIT HOZ A JÖVŐ?

A kiberterrorizmus potenciális veszélyének értékeléséhez és jövőjének meghatározásához szerintem érdemes az eddigiektől némileg eltérő megközelítést alkalmazni két alapvető kérdés megválaszolásával, miszerint: vannak-e olyan célpontok, amelyek sebezhetők a kibertámadásokkal szemben, valamint hogy vannak-e olyan terrorista csoportok, akik képesek és megfelelően motiváltak ilyen támadások végrehajtására? Úgy gondolom, hogy az első kérdésre a válasz egy magabiztos „igen". Számos tanulmány kimutatta, hogy a kritikus információs infrastruktúrák sebezhetők a kibertámadásokkal szemben, mivel rendkívül összetettek, és az eddigi példák alapján vélhetően még a „védettnek" tűnő rendszerekben is találhatunk sebezhető pontokat, végső esetben egy hozzáféréssel rendelkező személyen keresztül.

A második kérdésre már korántsem ennyire egyértelmű a válasz. A kiberhadviseléssel foglalkozó csoportok és a kiberbűnözői körök már bebizonyították, hogy képesek hozzáférni érzékeny információkhoz és magukhoz a létfontosságú rendszerelemekhez is. A terroristák elméletileg követhetnék ezen elkövetők példáját, és akár a tőlük szerzett eszközökkel eredményesen támadhatnának olyan célpontokat is, amelyek a jelenleg rendelkezésre álló eszközeikkel elérhetetlenek voltak, eddig ezekre azonban nem igazán volt példa. Úgy gondolom, hogy jelenleg a szükséges készségekkel és tudással rendelkező személyek nagyobb valószínűséggel használják fel ezen képességeiket és fegyvereiket az ellenségeik elleni kémkedésre, vagy a kiberbűnözéssel történő jelentős anyagi haszonszerzésre, mint arra, hogy kiberterrorista támadásokat hajtsanak végre. Ugyanakkor a trendek és a támadási képességek elvi lehetősége meglétének ismeretében a válasz sajnos szükségszerűen nem lehet egy egyszerű „kizárt". Sőt…

Indoklásképp érdemes röviden áttekinteni, hogy milyen jelenségek alapján vélem úgy, hogy a kiberterrorizmus által jelentett potenciális veszély miatti aggodalom megalapozott, és a közeljövőben kiemelt jelentőségű lehet. Annak érdekében, hogy a feltett kérdést megválaszolhassuk, a fentiek mellett érdemes röviden áttekinteni azokat a trendeket, amelyek formálják, illetve meghatározhatják az elkövetkezendő időszakot.

A potenciális célpontok számának növekedése

A jövőben számos terület válhat támadások lehetséges célpontjává. Gondoljunk például az önvezető járművekre, amelyek irányítását az ötödik generációs hálózaton keresztül kiberterrorista csoportok is befolyásolhatnák, vagy a gyógyszeripar

készítményeinek pontos összetételét tartalmazó adatbázisok távolról történő módosítására. Ugyanakkor lényegében felesleges szűkíteni a kört. Ebben az összefüggésben minél több eszköz és infrastruktúra függ a számítógépes hálózatok meglététől és helyes működésétől, annál sebezhetőbb lesz az ezt használó társadalom az esetleges támadásokkal szemben, és sajnos annál valószínűbb, hogy a terrorista csoportok hatékonyan fogják kihasználni az ilyen sebezhetőségeket.

> „Az információs dimenzióban folytatott terrorizmus által okozott kár pontosan mérhető, és egyre inkább egyenértékűvé válik a nehezebben kivitelezhető, több és körültekintőbb szervezést igénylő fegyveres támadásokkal. A nemzetközi szervezetek szerint növekszik az információs terrortámadások által elérhető célpontok száma is, mivel az internet használata egyre szélesebb körű a világon. Tehát belátható időn belül számolnunk kell azzal, hogy a terrorizmus a céljai elérése érdekében kihasználja az információs dimenzióban megvalósítható támadási módszereket és eszközöket, és az információs hadviselés teljes repertoárját alkalmazni fogja."[19]

A kiberfegyverek fejlődése

Az iráni nukleáris létesítmények vezérlőrendszerét támadó Stuxnet vírus és sok más egyéb, a fájlokat jellemzően egyszerűen törlő (úgynevezett „wiper") kártevő példáján láthattuk, hogy a felhasznált és így a nyilvánosság számára is megismerhető eszközök kiváló kiindulási alapot jelentenek a kiberfegyverek továbbfejlesztéséhez. A hacktivistáknak, a kiberbűnözöknek és az állami szereplőknek egyaránt érdeke az eszközök fejlesztése és egy részük bevetése is. Ezen kártevőket kielemezve és módosítva a megfelelő kompetenciával rendelkező terrorista csoportok lényegében minimális ráfordítással juthatnak az eddigieknél jóval hatékonyabb és a világ bármely részén bevethető fegyverekhez, amelyeket előbb-utóbb bizonyosan fel is fognak használni.

A súlypont áthelyeződése

Némileg paradox módon a hagyományos terrorizmus elleni fellépés sikere valószínűleg arra készteti a terroristákat, hogy egyre inkább az olyan, nem hagyományos fegyverek felé forduljanak, mint a kiberterrorizmus. Ugyan véleményem szerint például a gépjárművel végrehajtott, ramming típusú támadások vagy a hagyományos robbantások,

[19] Haig et al. 2009.

fegyveres merényletek jelenleg nagyobb fenyegetést jelentenek, mint a kiberterrorizmus, a közeljövőben ez könnyen megváltozhat. A fizikai korlátok megszűnése, a lényegesen egyszerűbb rejtőzködés és anonimitás, a szinte korlátlan próbálkozási lehetőségek, a potenciális célpontok sokszínűsége és óriási száma törvényszerűen eredményezi, hogy a terroristák a jövőben egyre inkább kiberterroristákká váljanak.

ÖSSZEGZÉS

A fentieket összegezve kijelenthetjük, hogy a kiberterrorizmus által jelentett potenciális veszély miatti aggodalom tehát megalapozott. Megvizsgálva a kiberterrorizmus történetét, megállapíthatjuk, hogy a különböző terrorszervezetek az információtechnológiát – és azon belül is elsősorban az internetet – kezdetben szinte kizárólag propagandacélokra használták. A 2010-es évektől a terrorista csoportok és más szélsőséges szervezetek egyre erőteljesebben, felkészültebben és nyíltabban használják a kiberteret eszméik hirdetésére, kiképzési célokra, kapcsolattartásra, toborzásra, működésük finanszírozására és nem utolsósorban pszichológiai hadviselésre. Bár a terrorszervezetek napjainkra egyre több számítógépes szakértővel rendelkeznek, ám még hiányzik a műszaki hátterük és vélhetően a kellő motivációjuk is ahhoz, hogy egy ország ellen átfogó információs támadást intézzenek.

Jelenleg a terrorista csoportok nagyobb valószínűséggel hajtanak végre támadásokat az egyszerűbb, könnyebben beszerezhető hagyományos fegyverekkel, mint hogy folyamatokat felügyelő és ellenőrző ipari vezérlők (Supervisory Control and Data Acquisition – SCADA) ellen indítsanak komplex támadásokat, amelyek félelem- és zavarkeltő képessége továbbra is bizonytalan. Ugyan a terroristák az utóbbi években egyre nagyobb mértékben használják az információs technológiát és a közösségi médiát, ezeket inkább a mindennapi működésük megkönnyítésére veszik igénybe, mintsem hogy támadások eszköze és célpontja legyen.

Ugyanakkor a kiberterrorizmus szinte bizonyosan a jövőnk része lesz. A kibertér további terjedése, az infrastruktúrák összefonódása, a célpontok számának és a kibertámadással okozható károk exponenciális növekedése szükségszerűvé teszi a kiberterrorizmus hasonló arányú növekedését is. Ahogyan a 2001. szeptember 11-ei események meglepték a világot, úgy a kiberterrorizmus is könnyen megteheti ugyanezt.

FELHASZNÁLT IRODALOM

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

Dornfeld László (2019): Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Budapest–Pécs: PTE ÁJK, 46–63.

Haig Zsolt et al. (2009): *A kritikus információs infrastruktúrák meghatározásának módszertana.* Budapest: ENO Avisory Kft. Online: https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.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), 30–36. Online: https://ctc.westpoint.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/

Kovacs, Eduard (2012): Hackers around the world: It's no TriCk, he's among the best in the world. *Softpedia,* 2012. február 18. Online: https://news.softpedia.com/news/Hackers-Around-the-World-It-s-No-TriCk-He-s-Among-the-Best-in-the-UK-253652.shtml

Nagy József (2017): Csányi Vilmos: A magyar politika azon siránkozik, hogy egyre kevesebben vagyunk, én inkább azon, hogy egyre hülyébbek vagyunk. *24.hu,* 2017. augusztus 10. Online: https://24.hu/kozelet/2017/08/10/csanyi-vilmos-a-magyar-politika-azon-sirankozik-hogy-egyre-kevesebben-vagyunk-en-inkabb-azon-hogy-egyre-hulyebbek-vagyunk/

National Research Council System Security Study Committee (1991): *Computers at Risk; Safe Computing in the Information Age.* Washington: National Academy Press.

Papp Zoltán István (2018): *A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái.* PhD-értekezés. Budapest: Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola.

Roberts, Paul (2012): Report: TeamPoison Hacker „TriCk" Pleads Guilty For Hacking Tony Blair's E-mail. *threatpost.com,* 2012. július 2. Online: https://threatpost.com/report-teampoison-hacker-trick-pleads-guilty-hacking-tony-blairs-e-mail-070212/76757/

Squatriglia, Chuck (2008): Polish Teen Hacks His City's Trams, Chaos Ensues. *wired.com,* 2000. január 11. Online: https://www.wired.com/2008/01/polish-teen-hac/

Egyéb források

Internet Usage Statistics [é. n.]: *The Internet Big Picture World Internet Users and 2022 Population Stats.* Online: https://www.internetworldstats.com/stats.htm

Office of Public Affairs U.S. Department of Justice (2016): *Ohio Man Sentenced to 20 Years in Prison for Plot to Attack U.S. Government Officers.* Online: https://www.justice.gov/opa/pr/ohio-man-sentenced-20-years-prison-plot-attack-us-government-officers