Berzsenyi Dániel – Ványi Rajmond

Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei – Az Iszlám Állam elleni magyar katonai szerepvállalás margójára

Az Iszlám Állam elleni magyar fellépés hosszas politikai előkészítést igényelt. Bár a döntés katonai erő alkalmazásáról szól, a terrorszervezet esetleges ellenlépései az Irakban szolgálatot teljesítő magyar katonák elleni fizikai támadásokon túl Magyarországra is veszélyt jelenthetnek – akár egy információs támadás formájában. Jelen tanulmánynak nem célja, hogy tippeket vagy ötleteket adjon, azonban fontosnak tartjuk egy olyan potenciális, a kiberbiztonságot veszélyeztető folyamat bemutatását, amelynek korai szakaszában nincs szükség komolyabb informatikai szaktudásra, nagy teljesítményű számítógépekre vagy speciális szoftverekre. A szerzők célja, hogy rámutassanak arra a nemzeti szintű kiberbiztonsági kitettségre, ami a döntéshozatal során ritkán kap megfelelő figyelmet.

Az Irakban kialakult helyzet[1] és a magyar szerepvállalás

A jelenlegi helyzet mozgatórugóit egészen a Szaddám-rezsimig követhetjük vissza, amelynek bukását követően a szunnitákat kiszorították a kormányzati hatalomból. A kisebbségben élő szunniták marginalizálódásához és végső soron az Iszlám Állam térnyeréséhez nagymértékben hozzájárultak az iraki kormány szunnitaellenes intézkedései. Így az utóbbi években például rendszeresen alkalmazta az Iraki Biztonsági Erőket arra, hogy szunnita politikai ellenfeleivel leszámoljon. 2013-ban több tömegdemonstrációt is a reguláris haderő bevetésével vertek le, az intézkedések több száz halálos áldozatot is követeltek.

2014 júniusában egy szunnita szélsőségesekből álló fegyveres csoport foglalta el Irak szunniták által lakott nyugati területeinek jelentős részét. A szélsőséges iszlamista terrorszervezet célja, hogy szír és iraki területeken egy Iszlám Kalifátust hozzon létre, azonban törekvéseiket soha nem látott brutalitás és erőszak kíséri. A felkelők jelentős sikereket értek el, amihez az Iraki Biztonsági Erők bénultsága nagymértékben hozzájárult.[2] Jelenleg az úgynevezett Iszlám Állam katonai képességei nehezen felbecsülhetők. A CIA szóvivője szerint 2014 őszén nagyjából 31 500 fegyveressel[3] rendelkezett a terrorszervezet, aminek közel kétharmadát tették ki a világ 90 országából összegyűlt külföldi harcosok.[4] A nem

1 Az Irakban kialakult helyzetről bővebben lásd Etl Alex: Irak belső válsága. *SVKK Nézőpontok,* 2014/1.

2 2011-től kezdődően az iraki miniszterelnök lett a haderő főparancsnoka, aki a parancsnoki struktúrát jelentősen átalakította. Az amerikai csapatok távozását követően az egyébként sem erős intézményi presztízzsel bíró haderő személyi állományában tapasztalható demoralizálódás a szervezet részleges felbomlásához vezetett. Etl Alex: i. m. 8–10. o.

3 Dilanian, Ken: CIA: Islamic State group has up to 31,500 fighters. *Associated Press,* 2014. 09. 11.

4 John O. Brennan CIA igazgató beszéde a Council on Foreign Relations rendezvényén, 2015. 03. 13.

sokkal később nyilatkozó kurd vezetők szerint a lázadók száma elérheti a 200 ezer főt,[5] miközben az orosz katonai vezetés 2014 decemberében 70 ezer főre becsülte a terrorszervezet bevethető fegyvereseinek számát.[6] Hasonlóan nehéz a felkelők által birtokolt haditechnikai eszközök és fegyverek felbecsülése is, az azonban biztosra vehető, hogy az Iraki Biztonsági Erők által hátrahagyott, valamint az egyéb zsákmányolt és vásárolt felszerelések között a gépkarabélyoktól, a mesterlövészfegyvereken, robbanószereken, páncéltörő és légvédelmi elhárító eszközökön túl nagy számban találhatók páncélozott harcjárművek, harckocsik, valamint logisztikai járművek és nehéztüzérségi eszközök is.[7] Bár sok a bizonytalanság az Iszlám Állam által bevethető harcosokra és eszközökre vonatkozó adatok tekintetében, az jól érzékelhető, hogy a szunnita lázadók katonai képességei jóval túlmutatnak egy hagyományos terrorszervezet lehetőségein. Mindez elsősorban azoknak a működésképtelen államoknak és cselekvésképtelenségüknek tudható be, amelyek az elmúlt időszak során alakultak ki az Iszlám Állam jelenlegi működési területén.

A terrorszervezetek esetében eddig soha nem látott katonai képességeken túl az Iszlám Állam olyan területeken is kitűnik, mint például a média használata. A különös kegyetlenséggel elkövetett erőszakos tetteiket, valamint a műkincsek és történelmi épületek, emlékhelyek rombolását akkurátusan megörökítő terrorszervezet szinte mindent azonnal elérhetővé tesz a világsajtó számára. A jól szervezett médiakampány nyomás alá helyezte és lépésre kényszerítette a nemzetközi közösséget, amelynek nyomán többek között Magyarország is katonákat küld Irakba. Az országgyűlési határozat[8] értelmében a magyar szerepvállalást a nemzetközi béke és biztonság előmozdítása, a terrorizmus elleni küzdelem és a nemzetközi köztelezettségek generálják. Utóbbi tekintetében az Országgyűlés hivatkozik az ENSZ Biztonsági Tanácsának 2014. augusztus 15-én és szeptember 24-én hozott határozataira (2170., 2178.), valamint az iraki kormány által az ENSZ tagállamaihoz intézett felkérésre. A terrorszervezet által elkövetett népirtás és emberiesség elleni bűncselekmények megakadályozására a Magyar Honvédség a nemzetközi koalíciós műveletek keretében partnerképesség-építési, őrző-védő és csapatkísérő feladatok ellátására alkalmas 150 – váltási időszakban 300 – fős kontingenst küld Észak-Irakba. Az erbili kiképző központ illetékességi területére települő magyar kontingens mandátuma 2017. december 31-ig szól.

A kiberterrorizmus vonzereje

Ahogyan a terrorizmusnak nincs nemzetközileg elfogadott, egységes meghatározása, úgy a kiberterrorizmus kapcsán sincs egyetlen széles körben elfogadott definíció. Az egyik legismertebb leírást Dorothy Denningnek tulajdonítják, aki szerint a kiberterrorizmus nem más, mint a kibertér és a terrorizmus konvergenciája. Az Egyesült Államok Hadi-

5 Cockburn, Patrick: War with Isis: Islamic militants have army of 200,000, claims senior Kurdish leader. *The Independent,* 2014. 11. 16.

6 Amint arról egy, az orosz vezérkari főnöknek tulajdonított nyilatkozat is beszámol: Islamic State formations comprise up to 70,000 gunmen – Chief of Russia's General Staff. *tass.ru,* 2014. 12. 10.

7 Blanchard, Christopher M.[et al: *The „Islamic State" Crisis and U.S. Policy*. Congressional Research Service, 2015. 05. 27.

8 Az Országgyűlés 17/2015. (IV. 17.) OGY határozata a Magyar Honvédségnek az Iszlám Állam elnevezésű terrorszervezet elleni nemzetközi fellépésben való részvételéről, *Magyar Közlöny*, 53. szám, 2015. április 17.

tengerészeti Posztgraduális Iskolájának professzor asszonya szerint „a kiberterrorizmus olyan jogellenes, számítógépek, hálózatok és az ezeken tárolt adatok elleni támadást jelent, amely alkalmas megfélemlítésre és kényszerítésre politikai vagy társadalmi célok elérése érdekében. Ahhoz, hogy egy támadás kiberterrorizmusnak minősüljön, személy vagy vagyon elleni erőszakot kell eredményeznie, vagy legalábbis a félelemkeltéshez elegendő kárt. A támadások következménye lehet halál, testi sérülés, robbanás vagy súlyos gazdasági veszteség. Kibertámadás érhet kritikus infrastruktúrákat, ugyanakkor a nem létfontosságú szolgáltatások működésének megzavarása vagy a csupán jelentős költségeket okozó támadások nem minősülnek kiberterrorizmusnak."[9]

Denning professzor asszony 2000 májusában a Fegyveres Testületek Bizottsága előtt tett felszólalása óta tizenöt év telt el. Napjainkban a hagyományos terrorizmus elleni intézkedések között a terrorizmus finanszírozását, a terrorista propaganda terjesztését, valamint a terroristák toborzását akadályozó intézkedések egyaránt megtalálhatók: e cselekmények online elkövetése ugyanúgy a terrorizmus támogatásának minősül, ezért a legtöbb ország jogrendszere ennek megfelelően szankcionálja az elkövetőket.

Fontos azonban különbséget tennünk az információtechnológia terrorista célú felhasználásának két iránya között. Az úgynevezett „hard" típusú felhasználás közé soroljuk a számítógépes hálózatokba történő felderítő vagy támadó célú behatolásokat, a kritikus infrastruktúrákat irányító információs rendszerek működésének megzavarását vagy blokkolását, illetve az elektronikai hadviselésben alkalmazott, nem halálos, rádiófrekvenciás fegyverekkel, nagy energiájú impulzusokkal végrehajtott támadásokat, melyek az információs rendszerek működésképtelenné tételére irányulnak. Ezzel szemben az információtechnológia „soft" alkalmazása jóval kiterjedtebb, és bár első pillantásra kevésbé tűnik veszélyesnek, a terrorszervezetek számára rengeteg lehetőséget biztosítanak a kapcsolattartásra, nézeteik terjesztésére, harcosok toborzására, különböző propagandatevékenységekre és támogatók szerzésére, illetve nyílt forrású felderítésre és információszerzésre.[10] Mindez elvezet bennünket ahhoz a szempontrendszerhez[11], amely a modern terrorista számára vonzóvá teszi a kiberterrorizmust.

1. *Költséghatékonyság.* A hagyományos terrorista módszerekhez viszonyítva a kibertér olcsóbb megoldásokat kínál a terroristák számára, hiszen nincs másra szükség, mint egy számítógépre és egy online kapcsolatra. Fegyverek és robbanószerek helyett számítógépes vírusokat hozhatnak létre és terjeszthetnek a különböző hálózatok felhasználásával.
2. *Anonimitás.* A kiberterrorizmus nagy előnye a hagyományos módszerekhez viszonyítva az anonimitás. A 2001 után elterjedt, nagy mennyiségű adat feldolgozásán alapuló, a hangsúlyt a megelőzésre fektető felderítő programok[12] ellenére az internet és az információtechnológia lehetőséget biztosít az azonosítás nélküli online tevékenységek végzésére. Ennek következtében a nemzetbiztonsági szolgálatok és

9 Weimann, Gabriel: Cyberterrorism How Real is the Threat? Special Report 119, United States Institute of Peace, 2004. december. 4. o.

10 Haig Zsolt – Kovács László: New way of terrorism: Internet- and cyber-terrorism. *AARMS,* 2007. 4. sz.

11 Weimann, Gabriel: Cyberterrorism: The Sum of All Fears?. *Studies in Conflict & Terrorism*, Routledge, 2005.

12 A globális felderítő programokról és hatásaikról lásd bővebben Lyon, David: Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society,* 2014. 07. 09.

a rendvédelmi erők nehezen tudják kideríteni a terroristák valódi személyazonosságát, mivel a kibertérben nincsenek az ellenőrzőpontokhoz vagy a határátkelőkhöz hasonló fizikai akadályok.

3. *Célpontdömping.* A kibertérben a célpontok változatossága és száma jelentős mértékben kibővül a terroristák számára. A kiberterrorista könnyen célba veheti kormányzatok, magánszemélyek, közművek, nagyvállalatok számítógépeit és hálózatait. A potenciális célpontok óriási száma és komplexitása garantálja, hogy a terrorista találni fog egy gyenge pontot vagy sérülékenységet, amit ki tud használni. Számos tanulmány és felmérés igazolja, hogy a kritikus infrastruktúrákat irányító információs rendszerek esetében összetettségük miatt lehetetlen minden gyengeséget felszámolni, ezért sebezhetők maradnak a terroristák által végrehajtott kibertámadásokkal szemben.
4. *Távoli támadás.* A hagyományos terrorista módszerekkel szemben további csábító tényező lehet a terrorszervezetek számára, hogy a kibertérben végrehajtott támadások távolról, személyes jelenlét nélkül megvalósíthatók. A távolból elkövethető akciók miatt a kiberterrorizmus kevesebb fizikai kiképzést, pszichológiai tréninget, halálos áldozatot és utazást, végső soron kevesebb ráfordítást igényel, miközben az új tagok és követők toborzása könnyebbé válik.
5. *Médiamegjelenés.* Az egyre kifinomultabb rosszindulatú szoftverek megmutatták, hogy a terroristák a kibertérben jóval szélesebb tömegeket tudnak közvetlenül elérni, és legtöbbször az esetleges cenzúra megkerülése sem jelent gondot. A hagyományos módszerekhez képest a kibertér lényegesen nagyobb média-megjelenést biztosít a terroristák számára, ami végső soron a legfőbb eszközük céljaik elérése érdekében.
6. *Sebesség.* A kibertérben az adatok hálózati sebességgel áramlanak, ami a terroristák számára az azonnali hatás kiváltását jelenti. Így egy hagyományos támadást valós időben képesek tudósítani a világ bármely pontjára, illetve egy kibertámadással akár a másodperc tört része alatt megzavarható egy számítógép, illetve számítógépes hálózat működése, miközben a terrorizmusellenes intézkedések nem alkalmasak, a terrorelhárító szervezetek pedig nincsenek felkészülve a hálózati sebességgel történő reagálásra.

Az Iszlám Állam kapcsán fent utaltunk rá, hogy a szervezet rendkívül hatékonyan alkalmazza a média eszközeit, ezen belül is kiemelkedő a közösségi média felhasználása, amivel a terroristák könnyen magukra vonják a nemzetközi sajtó figyelmét. Ennek eredményeként a terrorszervezet nemcsak katonai képességekben, de az online kommunikáció terén is sikeresen felülmúl minden más militáns csoportot. Bár történtek ellenlépések, amelyek keretén belül a Twitter internetes közösségi hálózatból eltávolították az Iszlám Államhoz köthető összes felhasználói fiókot, majd később a Diaspora és az orosz VKontakte rendszerében létrehozott, a terrorszervezethez köthető hozzáféréseket is felszámolták, a szunnita terroristák médiaelérése töretlen maradt.

Az Iszlám Állam által koordinált egyedülálló tartalom képes tömeges nézettséget generálni, amire jó példa az a 2014. március 17-én nyilvánosságra hozott felvétel, melyet 24 óra alatt 60 ezren néztek meg, majd két hónappal később egy 60 órás periódus alatt még

mindig több mint 800-szor osztották meg óránként. Ezek megdöbbentő számok, főleg ha figyelembe vesszük, hogy nem szokványos internetes tartalomról van szó, hanem brutális kivégzések és más kegyetlenkedések megörökítéséről. Azonban a terroristák nem érték be ennyivel, saját mobiltelefonos alkalmazásokat fejlesztettek a propaganda szélesebb körű terjesztésére, a szervezet által generált tartalmakat pedig olyan címkékkel látták el, melyek a legnépszerűbb keresőszavak alapján eltérítették és a terrorszervezet által generált tartalmakra irányították a felhasználókat.[13]

Jól érzékelhető, hogy az Iszlám Állam nagy jelentőséget tulajdonít, és ennek megfelelően komoly erőforrásokat fordít az online média és az internet által biztosított lehetőségek kiaknázására. Bár az internet- és információtechnológia alkalmazása – néhány kivételtől eltekintve – egyelőre kimerül a kapcsolattartásban, az ideológia terjesztésében, valamint tagok és támogatók toborzásában, nem zárható ki, hogy a kibertér által összekötött virtuális világban otthonosan mozgó szunnita lázadók szert tegyenek olyan kibertámadások kivitelezéséhez szükséges képességekre, amelyek más terrorszervezetekhez viszonyítva szintén egyedülállóak. Az ehhez szükséges anyagi források biztosítottnak tűnnek, mivel a terroristák bevételei egyes források szerint elérik a napi 1 millió dollárt,[14] míg más források alapján a napi 3 millió dolláros[15] jövedelem sem kizárt, amelynek nagy része az illegális olaj- és régiségkereskedelemből származik. További jelentős bevételi forrást jelentenek a terrorszervezet számára a váltságdíjakból befolyt összegek, melyek 2014-ben legalább 20 millió dollárt[16] tettek ki. Bár az Iszlám Állam költségvetésének kiadási oldaláról még kevesebb információ áll rendelkezésre, az említett anyagi háttérrel akár állami szintű kiberképességek kiépítése is finanszírozható lenne.

Magyarország egy kiberterrorista szemével

Egy hagyományos konfliktus során a stratégiai tervezők azokra a pontokra koncentrálnak, amelyek támadása vagy védelme valamilyen szempont alapján, például a földrajzi adottságok vagy nemzetgazdasági jelentőségük miatt kiemelten fontosak. Egy kiberkonfliktus esetén sincs ez másként, csak a kibertér esetében a stratégiai fontosságú pontok felderítéséhez nincs szükség hagyományos felderítő eljárásokra és hírszerző műveletekre, nem kell képezni és különleges eszközökkel ellátni a szakembereket. A ráfordítások (idő, pénz, szakértelem) túlnyomó része egy kibertámadás tervezésekor jelentős mértékben csökkenthető, és ha csak a célpontkiválasztásra koncentrálnak, akkor lényegében lenullázható.

Napjainkban egyetlen, csupán általános felhasználói ismeretekkel rendelkező terrorista néhány óra leforgása alatt képes feltérképezni Magyarország internetről elérhető összes nyitott hálózati portjának zömét, amihez elegendő egy teljesen átlagos számítógép. A portok jelentősége abban áll, hogy ezeken keresztül zajlik a kommunikáció a számítógépek között, ezeken keresztül érhető el egy számítógép távolról, emiatt a rendszerekért

13 Liste, Charles: Profiling the Islamic State. *Brookings Doha Center Analysis Paper,* No. 13, 2014. november.
14 Friedland, Elliot: The Islamic State. Special Report, The Clarion Project, 2015. május 10.
15 Laub, Zachary – Masters, Jonathan: The Islamic State. CFR Backgrounders, Council on Foreign Relations, 2015. május 18.
16 Cohen, David S.: Attacking ISIL's Financial Foundation. Remarks at The Carnegie Endowment For International Peace, 2014. október 23.

felelős szakemberek gyakran használják a hálózat biztonságának ellenőrzésére, akárcsak a rosszindulatú felhasználók a gyenge pontok feltérképezésére. Minden nyitott port egy potenciálisan kihasználható sérülékenységet tartalmazhat, függetlenül attól, hogy mi az adott port rendeltetése.

A számítógépek közötti kommunikációs portokat számozással különböztetik meg egymástól, amelyek számai a 0 és 65535 között vannak. A 0-ás és 1024-es számú portok közötti portokat „jól ismert" *(Well Known Ports)* portoknak is nevezik, melyeket az Internetes Számkiosztási Hatóság *(Internet Assigned Numbers Authority – IANA)* jelölt ki meghatározott célokra.

Nyitott hálózati portok magyarországon			
Port	Nyitott port (darab)	Név	Magyarázat
22	39 521	ssh	Távoli elérés (titkosított)
23	28 414	telnet	Távoli elérés (nem titkosított)
80	115 276	HTTP	Weblapok (nem titkosított)
443	65 144	HTTPS	Weblapok (titkosított)
3389	16 165	Remote Desktop Protocol	Távoli asztali elérés
ÖSSZESEN: 264 520			
SCADA portok (ipari rendszerek távoli vezérlése)			
502	1752	Modbus	Telemetriai adatok továbbítása
1089	1626	Foundation Fieldbus HSE	Alapszintű automatizálási hálózat
1541	2495	Foxboro/Invensys F. DCS Informix	Főként olaj- és gázipari elosztott rendszerfelügyelet
2222	5468	EtherNet/IP	Ipari hálózat (Ethernet és CIP technológiát kombinál)
5050	2212	Telvent OASyS DNA	Valós idejű, hálózati alapú ellenőrző rendszer
5450	1653	OSIsoft PI Server	Valós idejű adatfeldolgozás, elemzés és tárolás
10307	1748	ABB Ranger 2003	Ipari robot(kar)ok vezérlése
11001	1842	Johnson Controls Metasys N1	Ethernet/IP alapú automatizálási rendszer
13724	1754	ABB Ranger 2003	Ipari robot(kar)ok vezérlése
14592	1741	SCADA Node Secondary Port	Web alapú hozzáférés
19999	1794	DNP	Elosztott automatizálási kommunikációs protokoll

20000	2401	DNP3	Elosztott automatizálási kommunikációs protokoll
34962	1762	PROFINET	Komponens alapú automatizálási rendszer
34980	1751	EtherCAT	Ethernet alapú fieldbus rendszer
38589	1711	ABB Ranger 2003	Ipari robot(kar)ok vezérlése
38000	1755	SNC GENe	Villamosenergia-előállítás, -továbbítás, -elosztás
38600	1568	ABB Ranger 2003	Ipari robot(kar)ok vezérlése
44818	1598	EtherNet/IP	Ipari hálózat (Ethernet és CIP technológiát kombinál)
50001	2421	Siemens Spectrum Power TG	Villamos hálózatokat felügyelő és ellenőrző rendszer
62900	1569	SNC GENe	Villamosenergia-előállítás, -továbbítás és -elosztás
ÖSSZESEN: 40 621			
ÖSSZESEN: 305 141			

A táblázat jelmagyarázata: *22 (SSH):* Távolról történő, titkosított elérésre használják. Általában a viszonylag primitívnek számító „brute force" támadások ellen sem védik, ezáltal megfelelő idő- és anyagi ráfordítással a jelszó kitalálható, és hozzáférés szerezhető a rendszerhez. *23 (Telnet):* Szintén távolról történő, de nem titkosított elérésre használják. Utóbbinak köszönhetően a kommunikáció lehallgatható, nem védett a „man-in-the-middle (MitM)" és a „brute force" támadásokkal szemben. *80 (HTTP):* Weboldalak titkosítás nélküli elérésére használják. Lehallgatható, nem védett MitM jellegű támadásokkal szemben, ezért érzékeny adatok küldése a porton keresztül komoly problémákat okozhat. *443 (HTTPS):* Weboldalak titkosított elérésére szolgál, azonban ha a titkosítás nem megfelelő módon valósul meg, a kapcsolat visszafejthetővé válhat, ami a biztonságosnak vélt kommunikáció miatt fokozott veszélyeket rejt. *3389 (Remote Desktop Protocol):* Távoli asztali kapcsolat megvalósítása során használt port, amely védtelen a „brute force" jellegű támadásokkal szemben, ezáltal az alkalmazott jelszavak kitalálhatók kellő idő és anyagi ráfordítás esetén. *SCADA Portok:* Ipari folyamatirányító rendszerek portjai, gyakran kritikusinfrastruktúra-elemek működését szabályozzák, vezérlik távolról. A legnagyobb kockázatot az úgynevezett „nulladik napi" (zero-day) sérülékenységeken túl az jelenti, hogy korábban a SCADA rendszerek fejlesztésekor a biztonság nem tartozott az alapvető szempontok közé. (A táblázat a teljesség igénye nélkül a legfontosabb portokat és számukat adja meg a kihasználhatóság [támadhatóság] szempontjából.)

Fontos leszögeznünk, hogy a fenti táblázat pontossága nem száz százalékos, mivel feltételezésünk szerint minden port esetében az alapértelmezett beállítást használták, és ténylegesen az ennek megfelelő eszközök, illetve szolgáltatások kommunikálnak rajta, ami azonban a valóságban jelentősen eltérhet. Továbbá az internet folyamatos változása következtében a teszt megismétlése esetén nagy valószínűséggel más számokat kapnánk, ezért erre nem került sor. A kapott eredményeket trendeknek, hozzávetőleges értékeknek

tekintjük, amelyek alapján napjainkban Magyarországon több mint 300 000 darab nyitott port látható, illetve érhető el bárki – akár egy kiberterrorista – számára a világ bármely pontjáról.

Természetesen a nyitott portok száma nem tükrözi Magyarország sérülékenységének mértékét a kibertérben, ugyanakkor érdemes egy kis időt szentelni a számadatok és a potenciális veszélyek közötti összefüggések elemzésére. Több port esetében is megjelenik a „brute force" jellegű támadás kivitelezésének potenciális lehetősége, ami tulajdonképpen az összes lehetséges kulcs, vagy jelszó kipróbálásával határozza meg az éppen alkalmazásban levőt. Eredményessége – ahogyan arra az elnevezés is utal – kizárólag a rendelkezésre álló időtől és informatikai (számítási kapacitás) háttértől függ. Az ilyen jellegű támadásokkal szembeni védekezés elviekben megfelelő kulcsok és jelszavak (hosszúság, komplexitás) készítésével, illetve gyakori cseréjével könnyen megvalósítható. Ennek ellenére egy felhasználó átlagos jelszava az elmúlt évek során mindössze 6 karakterből és kisbetűkből állt, amit egy támadó nagyjából 3 perc alatt képes feltörni,[17] a jelszavak 61%-a több weboldalon is felhasználásra került, miközben a felhasználók 44%-a egy év alatt egyszer, vagy egyszer sem változtatta meg jelszavát.[18] Szintén több port esetén jelentenek veszélyt a „man-in-the-middle (MitM)", más néven közbeékelődéses támadások, melyek során a két számítógép közötti kommunikációs csatornát a támadó úgy téríti el, hogy mindkét gép számára a másik gépnek adja ki magát. Végül az egyik legnagyobb kockázatot jelentő biztonsági fenyegetés a „nulladik napi támadások" végrehajtása, amelyek olyan sérülékenységet használnak ki, amit nem hoztak nyilvánosságra, amiről a fejlesztő még nem tud, vagy még nem adott ki biztonsági javítást hozzá. 2014-ben 24 „nulladik napi" sérülékenységet publikáltak, ami 2006 óta a legmagasabb érték, miközben az 5 leggyakrabban kihasznált „nulladik napi" sérülékenység esetében egy év alatt 4 napról 59 napra nőtt a javítás kiadásához szükséges idő.[19] 2010-ben az iráni atomprogram szabotálására kifejlesztett Stuxnet 4 különböző „nulladik napi" sérülékenységet használt ki,[20] ami nagymértékben hozzájárult sikerességéhez.

A portokon keresztül kommunikáló vagy azokért felelős alkalmazásokat, akárcsak a hétköznapokból az átlagos felhasználó számára is jól ismert szoftvereket (irodai alkalmazásokat, operációs rendszereket, levelező klienseket) programozók készítik. A programozók munkájának, illetve a szoftverek minőségének mérésére több megoldás is létezik,[21] azonban az emberi hibákra vonatkozóan gyakran emlegetik a programsorok számához viszonyított 2%-os hibahatárt, ami nagyon jónak számít szakmai körökben.[22] Bár a nyitott portokon futó alkalmazások programsorainak számát még megbecsülni is nehéz, az egyértelmű, hogy jelentősen meghaladják a portok számát. Ha a programsorok tényleges számától elvonatkoztatunk, és azt feltételezzük, hogy minden nyitott port mögött csak egy programsor található, akkor a 2%-os hibahatárt a magyarországi nyitott portokra ve-

17 The Top Password Security Trends In 2014. *Cloudswave,* 2014. 09. 29.
18 Consumer Survey: Password Habits. *CSID,* 2012. szeptember.
19 Wood, Paul et al.: *Internet Security Threat Report*. Volume 20, Symantec Corporation, 2015. április.
20 Berzsenyi Dániel – Szentgáli Gergely: STUXNET: a virtuális háború hajnala. *biztonságpolitika.hu,* 2010. 10. 07.
21 Gyimóthy Tibor: Szoftverek minőségellenőrzése – A szoftverek is öregszenek? *Magyar Tudomány,* Magyar Tudományos Akadémia, 2013. 05. 12.
22 Panko, Raymond R.: Normal Program Development. 2008.

títve több mint 6100 olyan portot kapunk, amely szinte biztosan tartalmaz legalább egy kihasználható hibát vagy sérülékenységet. A hagyományos konfliktusokhoz hasonlítva ez azt jelenti, hogy legalább ennyi, támadhatóság szempontjából magas kockázatú pont van a kibertérben, amin keresztül magyarországi szolgáltatások és infrastruktúrák működése megzavarható vagy leállítható.

Ennél a logikánál maradva, ha egy terrorista szervezet komolyabb károk okozását szeretné elérni, akkor az ipari folyamatirányító rendszerekre szűkítve a kört még mindig több mint 800 olyan portot fog találni, amelyeket távolról elérve legalább egy még fel nem fedezett vagy javítatlan hibára találhat, aminek kihasználásával hozzáférést szerezhet a rendszerhez. Az ipari folyamatirányító rendszerekben nagy számban előforduló programozható logikai vezérlők *(programmable logic controller – PLC)* és elosztott vezérlő rendszerek *(distributed control system – DCS)* tekintetében azonban közelebb kerülünk a valódi fenyegetés mértékéhez, ha az ezekben átlagosan előforduló 30-150 sérülékenységgel számolunk.[23] Ilyen – a PLC-khez használt – kommunikációs protokoll a táblázatban is szereplő Modbus, amely 1752 darab nyitott porttal rendelkezik Magyarországon. Bár nem minden hiba és sérülékenység használható ki távoli elérésen keresztül, viszonyítási alapként érdemes a PLC-k legalacsonyabb sérülékenységi mutatóját megszorozni a nyitott Modbus-portok számával. Ez hozzávetőlegesen 52 560 sérülékenységet feltételez egyetlen ipari folyamatirányító rendszer esetében, amiből a lehetséges célpontok feltérképezésének eredményét tartalmazó táblázatban 20 található. Óvatos becsléssel is milliós nagyságrendű tehát ma Magyarországon azoknak a sérülékenységeknek a száma, amelyek nukleáris és hőerőműveket, vízellátó rendszereket, olajfinomítókat vagy éppen vegyi üzemeket, azaz kritikus infrastruktúrákat irányító információs rendszerekben találhatók.

Összegzés

A magyarországi nyitott hálózati portok feltérképezéséhez egyetlen számítógépet és egy az internetről szabadon elérhető úgynevezett „portscanner" programot használtunk, amelynek alkalmazása nem igényel informatikai előképzettséget, a szoftver alkalmazásához szükséges ismeretek szintén elérhetők az internetről. Feltételezésünk szerint egy, a kibertérből érkező támadás esetén az első lépésben a magyarországi nyitott portok – minimális ráfordításokkal megvalósítható – feltérképezésére kerülne sor, ami a célpontkiválasztás elsődleges eszközeként szolgál. Elemzésünk kizárólag a portok támadhatóságának feltérképezésére irányult, így nem terjedt ki más módszerekkel történő kombinált alkalmazásra, vagy például az alkalmazási rétegben elkövethető támadások vizsgálatára.

A valóságban a portok számánál a kihasználható sérülékenységek száma jelentősen magasabb, ami egzakt értékek nélkül is bőséges célpontlista összeállítását teszi lehetővé egy kibertámadás kezdeti fázisában mindössze 4 és fél óra alatt. A lehetséges célpontok felkutatásához szükséges idő egy tényleges támadás előkészítésének csupán töredéke, az előkészítés pedig gyakran olyan passzív folyamat, aminek a felderíthetősége alacsony. Ezzel szemben egy megfelelően tervezett támadás rendkívül gyors és aktív folyamat, ezáltal az észlelés is könnyebb.

23 Byres, Eric: SCADA Security: Welcome to the Patching Treadmill. *Tofino Security,* 2013. 03. 14.

A felfedezett sérülékenységek kihasználása már komolyabb informatikai ismereteket, illetve eszközöket és anyagi ráfordítást igényel, azonban ezeknek a kifejlesztésével nem feltétlenül kell törődnie egy terrorszervezetnek, ha ezeket a piacról is be tudja szerezni. Napjainkban a „nulladik napi" sérülékenységekre vonatkozó információk beszerzése vagy hackercsoportok felbérlése nem sokban különbözik a fegyver- vagy kábítószer-kereskedelemre jellemző eljárásoktól. Megfelelő anyagi források birtokában az alvilág kibertérre specializálódott szegmensében szinte minden megvásárolható, amire a célpontkiválasztást követően szükség lehet egy kibertámadás végrehajtásához.

Az Iszlám Állam interneten folytatott ismert tevékenysége csak néhány esetben értékelhető kibertámadásnak, azonban ezek sem okoztak jelentős károkat Magyarországon, mivel jellemzően alacsony látogatottságú, kritikus folyamatokat nem kezelő honlapok megtámadásáról van szó.[24] Bár hazánk esetében az sem bizonyított, hogy valóban az Iszlám Állam követte el a honlapok feltörését, fontos azt is szem előtt tartani, hogy a támadások főként ingyenes tartalomkezelő rendszereket értek, amelyeket biztonsági szempontból gyakran elhanyagolnak, ezáltal a sérülékenységek felderítéséhez és kihasználásához nem feltétlenül szükséges komoly szaktudás. (Határainkon túl a leginkább figyelemre méltó, ismert támadást az Amerikai Egyesült Államok Központi Parancsnokságának [CENTCOM] közösségimédia-felületei ellen hajtotta végre az Iszlám Állam.)[25]

Fontos megjegyezni, hogy az egyes szervezetek közösségi felületei ellen végrehajtott sikeres támadások nem azonosak a közvetlen támadásokkal. A közösségimédia-szolgáltatásokon keresztüli támadások többnyire ugyanúgy az ideológia terjesztését szolgálják, mint az Iszlám Állam saját fejlesztésű, azonos célú felületeinek működtetése. Visszakanyarodva a kiberterrorizmus vonzerejéhez, ez nem más, mint az információtechnológia „hard" típusú alkalmazása „soft" típusú célok elérése érdekében. Az biztos, hogy az ideológia terjesztésére irányuló támadásokat felválthatják a tényleges, fizikai károkkal járó kibertámadások, ugyanakkor felmerül a kérdés, hogy egy terrorszervezet szempontjából a felszámolására irányuló katonai műveletben történő részvétel elegendő alapot szolgáltat-e arra, hogy fizikai pusztítással járó kibertámadást indítson a műveletben résztvevő országok ellen. A terrorista szervezetek szempontjából a hagyományos hadviselésben is kimutatható, a kiberhadviselés kapcsán azonban még jelentősebb aszimmetria olyan lehetőségeket és eszközrendszert kínál, aminek alkalmazása inkább csak idő kérdése.

24 Sorra töri fel a magyar oldalakat az Iszlám Állam hackere. *origo.hu,* 2015. 04. 08., és Iszlám fanatikus támadhatta meg az Óbudai Egyetem honlapját. *origo.hu,* 2015. 05. 19.

25 Central Command Twitter account apparently hacked by CyberCaliphate. *rt.com,* 2015. 01. 12.