HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

PÉNZVÁLTÓ NIKOLETT[1]

Kritikus információs infrastruktúrák kibertámadások elleni védelme Törökországban: kiberbiztonság *versus* internetszabadság?

Protecting Critical Information Infrastructures from Cyber Attacks in Turkey: Cybersecurity *versus* Internet Freedom?

Absztrakt

A tanulmány Törökország kiberbiztonsági környezetét, fő szereplőit, intézményeit és stratégiáit mutatja be. Az elemzés rámutat a globális trendek, a növekvő regionális instabilitás, a török belpolitikai fejlemények és a török kibervédelmi képességek közötti összefüggésre. Emellett felhívja a figyelmet arra, hogy az államok kibervédelmi képességeinek fejlesztése megfelelő jogi garanciák hiányában nem csak a kiberbűnözők és a kiberterroristák elleni harcot könnyíti meg az autoriter rezsimek számára, hanem a politikai ellenvélemények elhallgattatását is.

Kulcsszavak: Törökország, kiberbiztonság, internetszabadság

Abstract

The study introduces Turkey's cybersecurity environment, main actors, institutions and strategies. The analysis highlights the connection between global trends, the growing regional instability, the Turkish internal political affairs and the development of the Turkish cyber defense capabilities. The paper draws attention to the fact that without proper legal guarantees the development of the states' cyber defense capabilities can make it easier for authoritarian regimes not just to fight against cybercriminals and cyberterrorists but to silence the political opposition.

Keywords: Turkey, cyber security, internet freedom

[1] Nemzeti Közszolgálati Egyetem − National University of Public Service; E-mail: penzvalto.nikolett@uni-nke.hu; ORCID: 0000-0002-1114-1488

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

BEVEZETÉS

Az elmúlt években felértékelődött a kiberbiztonság szerepe a török biztonságfelfogásban (is). Okai között az általános világpolitikai trend mellett szerepet játszottak a török belpolitikai fejlemények, valamint a feszültségek növekedése Törökország közvetlen földrajzi környezetében. A török kiberbiztonsági intézményrendszer folyamatos fejlődése mellett ezt támasztja alá az is, hogy bár a török nem egy „stratégiaalkotó nemzet", 2016-ban mégis már a második kiberbiztonsági stratégiát fogadták el, amit nyilvánosan, angol nyelven közzé is tettek.

Jelen tanulmány célja kettős: egyrészt, hogy áttekintést nyújtson Törökország biztonságának kiberszektoráról; másrészt, hogy rámutasson azokra a morális aggályokra ezen összefüggésben, melyek a jelenlegi, rendkívüli mértékben biztonságiasított török politikai környezet jellegéből fakadnak.

A NATO-tag Törökország geopolitikai és geostratégiai feszültségek középpontjában áll.[2] A Szövetség számára ezért is kiemelten fontos a törökországi kiberviszonyok ismerete, különösen miután 2014-ben a kibertámadás bekerült a washingtoni szerződés kollektív védelmet előhívó 5. cikkelyének hatálya alá.

TÖRÖKORSZÁG ÉS A KIBERBIZTONSÁG

Törökország 2016-ban 46 millió fővel a 14. legtöbb internetfelhasználóval rendelkezett a világ országai közül.[3] Az internet-penetráció tekintetében azonban korántsem birtokolt ennyire előkelő helyezést: lakosságának mindössze 58%-a bírt hozzáféréssel az internethez.[4] Különböző statisztikák adatai szerint világszinten a kibertámadásoknak egyik legkitettebb ország. Az amerikai FireEye kimutatása alapján 2016-ban Törökországban több célzott malware-támadást észleltek, mint egész Európában összesen.[5] Az egyik török védelmi cég, az STM (*Savunma Teknolojileri Mühendislik ve Ticaret* A. Ş.) jelentése a 9. helyre rangsorolja az országot a legtöbb kibertámadást elszenvedő országok listáján.[6] A török napilap *Daily Sabah* szerint Törökország 2017-ben 90 millió kibertámadást szenvedett el. A cikk kiemeli, hogy a támadások száma a 2016. júliusi törökországi puccskísérlet után meg-

[2] Egyetlen példát kiemelve: azt követően, hogy átmenetileg elhidegült a török−orosz viszony − miután a szíriai háború részeként a török légierő F−16-os repülőgépe 2015. november 24-én lelőtt egy Szu−24-es orosz vadászbombázót −, a két állam között több kiber-incidensre is sor került. 2016. december 7-én egyórás, úgynevezett túlterheléses támadás érte a Sputnik Türkiye weboldalát; illetve 2016. január elején török hackerek (Börtecine Cyber Team) feltörték az orosz kommunikációs miniszter Instagramját. Turkish hackers break into Russian minister's Instagram account, 2016. 01. 03. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)

[3] Internet Users by Country (2016). internetlivestats.com (A letöltés dátuma: 2018. 05. 07.)

[4] Uo.

[5] Chris Bing: Why Turkey, a NATO ally, is a huge target for malware, 2017. 02. 03. cyberscoop.com (A letöltés dátuma: 2018. 05. 07.)

[6] Turkey ninth most targeted by cyberattacks, 2016. 02. 08. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)

sokszorozódott.[7] Egy másik helyen egy török tisztviselő úgy nyilatkozott, Törökország az Egyesült Államok és Brazília után a világon a harmadik támadásoknak leginkább kitett ország, évi közel 25 millió kibertámadással.[8]

AZ ELMÚLT ÉVEK NAGYOBB ELSZENVEDETT KIBERTÁMADÁSAI

Az elmúlt években Törökországot számos jelentős kibertámadás érte. 2012 júliusában például a Török Külügyminisztérium honlapját törte fel politikai indítékból a török kormányellenes RedHack Csoport. A támadás során 65 gigabájtnyi belső fájlt szereztek meg, illetve kiszivárogtattak a török külügyi hatóságok által külföldi diplomatáknak kiadott személyazonosító igazolványok adatait.[9] 2016 februárjában a török rendőrség rendszerét törte fel a The Cthulhu nicknevet viselő elkövető, szintén politikai okokból. Több millió török állampolgár mintegy 17,8 gigabájtnyi szenzitív személyes adatát töltötte le, majd tette közzé.[10] 2016 decemberében pedig Berat Albayrak energiaügyi miniszter megerősítette, hogy az isztambuli áramkimaradásokat szintén külső támadás okozta.[11]

Az eddigi legjelentősebb támadásra 2015 decemberében került sor. Az Anonymus[12] által felvállalt támadás indítékaként az a vád szolgált, miszerint Törökország a kőolajvásárláson keresztül, valamint fegyverekkel támogatja az „Iszlám Államot" a szíriai harcokban. A török médiában megjelent spekulációk az oroszokat gyanították a támadás mögött.[13] A tíz napon keresztül tartó, úgynevezett túlterheléses (*Distributed Denial of Service,* DDoS) támadás mintegy 400 ezer, ‚.tr' domainnel végződő török weboldalt tett hozzáférhetetlenné. Ez magában foglalta szinte az összes kormányzati oldalt, de érintette a török bankrendszert is, ellehetetlenítve például az online tranzakciókat. A 40 gigabit / másodperces támadás közvetlenül a szolgáltató Türk Telekom szervereit blokkolta, ezért lehetett ilyen sikeres.[14]

[7] Bariş Şimşek: Turkey to prop up cyber defense with new law, 2017. 07. 06. dailysabah.com (A letöltés dátuma: 2018. 05. 07.)
[8] Cyberattacks against Turkey increase sharply, 2017. 12. 02. trtworld.com (A letöltés dátuma: 2018. 05. 07.)
[9] RedHack discloses IDs of foreign diplomats in Turkey, 2012. 07. 03. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
[10] Jason Murdock: Anonymous: Hacker unleashes 17.8GB trove of data from a Turkish national police server, 2016. 02. 16. ibtimes.co.uk (A letöltés dátuma: 2018. 05. 07.)
[11] Major cyber-attack on Turkish Energy Ministry claimed, 2016. 12. 31. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
[12] Anonymous - Message to Turkey [Those who support ISIS], 2015. 12. 23. youtube.com (A letöltés dátuma: 2018. 05. 07.)
[13] Lásd például Turkey under cyberattack by Russia: *Report,* 2015. 12. 17. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
[14] Ahmet Sabanci: Did a single hacker − not Anonymous − cripple Turkey's Internet?, 2015. 12. 28. dailydot.com (A letöltés dátuma: 2018. 05. 08.)

TÖRÖK HACKTIVISTA ÉS HACKERCSOPORTOK − TÖRÖKORSZÁG MINT A KIBERTÁMADÁSOK FORRÁSA

Az Akamai informatikai cég értékelése szerint 2016 első negyedévében és 2017 második negyedévében is Törökország volt a 3. legnagyobb forrása a kibertámadásoknak a világon, Kína és az Egyesült Államok után.[15] Ezért mindenképpen indokolt röviden áttekintenünk a jelentősebb törökországi hacker-, illetve hacktivista csoportokat is.

A RedHack csoport küldetésnyilatkozata szerint céljuk egy egyenlő, igazságos és kizsákmányolástól mentes világ megteremtésének támogatása. 2012–2013-ban deface támadást (honlaprongálás) hajtottak végre kis túlzással az összes állami szerv weboldala ellen, emellett főként adatszivárogtatások jellemzik a tevékenységüket.

A B3yaz Hacker nevű szerveződés tevékenysége két csoportra osztható: egyrészt sebezhetőségi teszteket (Pentesteket) végeznek, másrészt értékeikkel ellentétes tartalmú oldalakat támadnak.[16]

A Turk Hack Csapat az egyik legismertebb és legjobban szervezett hacktivista társaság. Öndefiníciójuk szerint tagjaik „Muszlimok, akik szeretik a hazájukat". Jelentősebb támadásaik között említhető a *The New York Times,* illetve a *The Guardian* honlapja elleni akció, melyeket a török elnök kritizálása miatt hajtottak végre; de feltörték a Szentszék weboldalát is, miután a pápa népirtásként hivatkozott az 1915-ös örmény tragédiára.

A Türk Güvenliği ideológiája nem egyértelmű, a jelek szerint egy nacionalista csoport. Nemzetközi támadások kötődnek hozzájuk, például a fuse.microsoft.com, a The Register és a Vodafone ellen.

Az Ayyıldız Csoport tagjai „patrióták", akik támadásaikat általában az állam céljaival párhuzamosan hajtják végre.

A Cyber Warrior (Akıncılar) csoport bizonyítékok szerint szoros kapcsolatot ápol a török állammal és rendőrséggel. Közleményeik szerint nem támadnak török weboldalakat. Hajtottak már végre támadást többek között Izrael, Örményország, Egyiptom és Ausztria ellen.

Végül érdemes megemlítenünk a Kurdisztáni Munkáspárthoz (PKK) köthető PKK Hack Teamet, akikhez a Zone-H weboldal 279 deface támadást köt.[17]

TÖRÖK KIBERBIZTONSÁGI INTÉZMÉNYRENDSZER ÉS STRATÉGIÁK

A török kiberbiztonsági szervezet- és intézményrendszer csúcsán politikai döntéshozó szervként a Közlekedési Tengerészeti és Kommunikációs Minisztérium (*Ulaştırma Denizcilik ve Haberleşme Bakanlığı,* a továbbiakban UDH) áll. A telekommunikációs szektor szabályozó hatósága az Információs- és Kommunikációs-technológiai Hatóság (*Bilgi Tek-*

[15] Q4 2017 State of the Internet Security Report. akamai.com (A letöltés dátuma: 2018. 05. 07.)
[16] A Zone-H összesítése szerint 540 defacement kötődik bizonyíthatóan hozzájuk, főként 2015-ből. Zone-H.org (A letöltés dátuma: 2018. 05. 07.)
[17] Salih Bıçakcı, Doruk Ergun, Mitat Çelikpala: The Cyber Security Scene in Turkey. In Sinan Ülgen, Grace Kim (szerk.): A primer on cyber security in Turkey: and the case of nuclear power. 2015, 22−51.

nolojileri ve İletişim Kurumu, a továbbiakban BTK), amely olyan feladatokat lát el, mint az engedélyezés, felügyelet, fogyasztói jogok védelme, versenyszabályozás, technikai előírások megalkotása vagy a spektrum-menedzsment.[18] A 2016. júliusi törökországi puccskísérletet követő („gülenista" vádak miatti)[19] megszüntetéséig a telekommunikációs eszközökön keresztül végrehajtott jelinformációk és kommunikáció felügyeletét, nyomon követését, értékelését és rögzítését, valamint az internetes tartalom és szolgáltatók szabályozását a BTK alá rendelt Telekommunikációs Elnökség (*Telekomünikasyon İletişim Başkanlığı,* TİB) látta el. A kritikus infrastruktúra védelmében, különösen a válságkezelésben kiemelt szerepe van a Katasztrófa- és Vészhelyzet-kezelési Elnökségnek (*Afet ve Acil Durum Başkanlığı,* a továbbiakban AFAD). Katasztrófák esetén (melynek két típusát különítik el a török jogszabályok:[20] természeti és technológiai katasztrófákat) az AFAD a fő koordináló szerv, ami közvetlenül a miniszterelnök irányítása alatt áll. Ki kell emelnünk továbbá a 24/7-ben működő TR-CERT (török nevén *Ulusal Siber Olaylara Müdahale Merkezi,* a továbbiakban USOM) szerepét. A török kiberbiztonsági célkitűzések között szerepel, hogy minden állami intézmény, illetve kritikus infrastruktúrát üzemeltető magánvállalat rendelkezzen továbbá saját Szektorális Kiber-incidenskezelő Csapatokkal (*Siber* Olaylara Müdahale Ekipleri, a továbbiakban SOME). A SOME-k működését, az USOM, létrehozását az UDH koordinálja. 2015 januárjáig 245 intézményi SOME megalakítására került sor, melyeket 720 fő személyzettel töltöttek fel. A katonai szektort illetően a legfontosabb kibervédelmi szerv a 2013 óta működő Török Fegyveres Erők Kibervédelmi Parancsnoksága. Emellett Törökország 2016 óta rendelkezik Cyber Fusion Központtal is.[21]

2012. október 20-án a 2012/3842 számú kormányhatározat (A nemzeti kiberbiztonsági erőfeszítések implementációja, menedzselése és koordinálása) hozta létre a Kiberbiztonsági Tanácsot, mely 2013-ban elkészítette az első török kiberstratégiát, a Nemzeti Kiberbiztonsági Stratégia és 2013–2014 Akcióterv elnevezésű dokumentumot. A Kiberbiztonsági Tanács elnöke az illetékes miniszter, tagjai között pedig helyet kapnak többek között államtitkárok a kül- és belügyminisztériumból, a vezérkar, valamint a nemzetbiztonsági szervek képviselői, illetve a Török Tudományos és Technológiai Kutatási Tanács (TÜBITAK) és a BTK elnöke.

A 2013-as kiberstratégia kiemelt hangsúlyt fektet a kritikus infrastruktúra, a humán tőke és a hazai technológia fejlesztésére. Hiányosságként emeli ki a szakemberek és megfelelő infrastruktúra, a koordináció hiányát, valamint a törvényi szabályozás elégtelenségét. A dokumentum 29 különálló intézkedési javaslatot sorol fel, melyek között szerepel például K+F laborok létrehozása az egyetemeken; egy olyan teszt-infrastruktúra kifejlesztése és telepítése, amely a kulcsfontosságú állami szervezetek adatvesztésének felderítésére

[18] Bıçakcı et. al.: i. m.
[19] Turkey shuts down telecommunication body amid post-coup attempt measures, 2016. 08. 17. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
[20] Lásd a 2009. évi 5902. számú törvény definícióit: Afet Ve Acil Durum Yönetimi Başkanliğinin Teşkilat Ve Görevleri Hakkinda Kanun. ecolex.org (A letöltés dátuma: 2018. 05. 07.)
[21] Bıçakcı et. al.: i. m.

szolgál; illetve a Török Nyelvi Szövetség megbízása egy kiberbiztonsági fogalmakat tartalmazó szótár megalkotásával.[22]

A 2013-ast követő, 2016-ban elfogadott „Nemzeti Kiberbiztonsági Stratégia 2016−2019" felépítését tekintve négy fő részre tagolódik: 1. Bevezetés, 2. Elvek, 3. Kiberbiztonsági kockázatok, 4. Stratégiai kiberbiztonsági célkitűzések és intézkedések. A dokumentum alkotói felismerik, hogy az abszolút kiberbiztonság napjainkban már nem elérhető, ezért a cél ehelyett a kiberbiztonsági kockázatok kezelhető és elfogadható szinten tartása. A stratégia explicit módon kimondja, hogy a kiberbiztonság a nemzeti biztonság integráns része. Az egyes kockázatok értékelése előtt a dokumentum megfogalmazza, hogy más országok stratégiai dokumentumainak vizsgálata alapján a potenciális kiberbiztonsági kockázatok és alapelvek nem térnek el jelentősen az egyes országok között. E megállapításra hivatkozva, illetve tekintettel elemzésünk fókuszára, a következő fejezet relevanciája szempontjából a stratégiában említett kockázatok és célkitűzések közül itt mindössze egyet-egyet emelünk ki. A kiberbiztonsági kockázatok között negyedik pontként említi a dokumentum a „különböző intézmények és szervezetek reputációjának megsértését"; a célkitűzések fejezet 18. pontja pedig kiemeli az anonimitás megszüntetésének (eliminate) célját.[23]

HACKER, HACKTIVISTA, KIBERTERRORISTA; BŰNÖZŐ VAGY ÁLLAMPOLGÁR? – MORÁLIS AGGÁLYOK A TÖRÖK JOGI ÉS POLITIKAI KÖRNYEZET TÜKRÉBEN

Közhely, hogy a biztonság és szabadság közötti megfelelő egyensúly megtalálása nem könnyű feladat. A kibertámadások elleni védekezés kapcsán is felmerül, hogyan lehet hatékonyan fellépni a támadók ellen úgy, hogy közben ne korlátozzuk a szükségesnél jobban az internethasználó állampolgárok jogait? Kérdéseket vet fel az is, hol húzódik a határvonal hacktivizmus (politikai aktivizmus) és (kiber)terrorizmus között?

A kibertér Törökországban a kormánypárt és a tevékenységét kritizáló állampolgárok közötti küzdelem egy újabb színterévé vált. Ahhoz azonban, hogy megértsük ennek a kijelentésnek a jelentőségét, legalább nagy vonalaiban ismernünk kell a jelenlegi török politikai és jogi környezetet. Különböző nemzetközi szervezetek régóta kritizálják Ankarát a török terrorizmus elleni törvény rendkívül kiterjesztő terrorizmus-értelmezése miatt. Terrorizmusnak számít például minden olyan cselekedet, aminek célja a Köztársaság az alkotmányban meghatározott (politikai, jogi, társadalmi, gazdasági és szekuláris) jellegének megváltoztatása, az állam oszthatatlan (területi, nemzeti) egységének megkárosítása, az államhatalom meggyengítése vagy megragadása. Külön szabályozás vonatkozik a terrorizmus pártolóira. Az egyik leggyakoribb vád a szintén tágan értelmezett „terrorizmus párti propaganda" folytatása.[24] Törökország valóban sokat szenvedett a terrorizmustól az utóbbi években. A

[22] National Cyber Security Strategy and 2013-2014 Action Plan. enisa.europa.eu (A letöltés dátuma: 2018. 05. 07.)
[23] National Cyber Security Strategy 2016−2019. udhb.gov.tr (A letöltés dátuma: 2018. 05. 07.)
[24] A jogszabály szövege török nyelven: Terörle Mücadele Kanunu, 1991. mevzuat.tr (A letöltés dátuma: 2018. 05. 07.)

Global Terrorism Database adatai szerint 2016-ban 540 terrormerényletben 1004 ember halt meg.[25] A 2016. júliusi törökországi puccskísérletet követően megkezdődött letartóztatási hullám volumene azonban mégis politikai motivációt (is) sejtet. Nem egészen két év alatt több mint 77 ezer embert tartóztattak le, és mintegy 152 ezer embert bocsátottak el az állásából terrorizmus vádja miatt.[26] A török politikai-jogi környezet felvázolásakor még egy jogszabályt mindenképpen ki kell emelnünk: akár négyéves börtönbüntetésre is ítélhető az, aki megsérti az elnök (jelenleg, 2014 óta Recep Tayyip Erdoğan) személyét. Az elnök megsértéséért indított perek száma 2015-ben elérte az 1953-at.[27]

A Freedom House 2017-es *Freedom on the Net* című jelentése Törökországot a „nem szabad" kategóriába sorolja. A jelentés a hozzáférés, a tartalomkorlátozás és a felhasználói jogok szempontjából értékeli az egyes államokat.[28]

A török hatóságok hatékonyan alkalmazzák eszközként az internethez való hozzáférés akadályozását. Az egyes korlátozások bevezetésének időzítésből kitűnik a politikai motiváció. Gyaníthatóan többnyire azért éltek ezzel az eszközzel, hogy megakadályozzák a lakosság önszerveződését és ellenállását. 2016. szeptember 11-én például hat órán keresztül, tíz délkelet-törökországi városban (12 millió embert érintve) felfüggesztették a telefon- és internet-szolgáltatást. Minderre azt követően került sor, hogy 28 kurd kormányzót eltávolítottak a pozíciójából. Egy hónappal később tizenegy városban több napra felfüggesztették az internet-szolgáltatást. A lépés egybeesett a kurd politikusok letartóztatása miatti tömegtüntetésekkel valószínűleg azzal a szándékkal, hogy megakadályozza, illetve késleltesse a rendőri fellépés mikéntjéről való tudósítást. A „hozzáférés akadályozása" kategóriát a Freedom House jelentése Törökország esetében 25-ből 13 pontra értékelte, ahol minél magasabb az érték, annál kevésbé számít egy terület „szabad"-nak.[29]

A „tartalomkorlátozás" területén 35-ből 23 pontra értékelték az országbeli viszonyokat. Ankara rendszeresen blokkolja a hozzáférést bizonyos weboldalakhoz. 2016 novemberében hozzávetőlegesen 114 ezer weboldal nem volt elérhető. 2016 folyamán legalább 7 alkalommal került sor a Facebook, a Twitter, illetve a YouTube blokkolására. Az időzítés többnyire itt is köthető valamilyen politikailag érzékeny eseményhez, például terrortámadásokat, letartóztatásokat követően került sor a tiltó kormányzati lépésekre. Az internetes tartalmak szabad elérését tovább akadályozandó, 2016 novemberében a BTK elrendelte több, mint 10 VPN szolgáltatás (*Virtual Private Network*), köztük a Tor betiltását. 2017 májusában pedig sor került a Wikipedia blokkolására is. A tilalmat az ankarai büntetőbíróság hagyta jóvá, hogy megakadályozza a hozzáférést két, Törökország szíriai szerepvállalásáról szóló, a török hivatalos narratívától eltérő tartalmú cikkhez. A hozzáférés akadályozásán felül a török kormány esetenként tartalmak eltávolítását is kezdeményezi. 2016

[25] Ez a szám tartalmazza a júliusi puccskísérletben életüket vesztettek számát is.
[26] Turkey Purge. turkeypurge.com (A letöltés dátuma: 2018. 05. 02.)
[27] ECHR (2016): European Court of Human Rights Judgment in the Case of Artun and Güvener v. Turkey. aihmiz.org.tr (A letöltés dátuma: 2018. 04. 12.)
[28] Freedom on the Net 2017, Turkey. freedomhouse.org (A letöltés dátuma: 2018. 05. 07.)
[29] Uo.

második felében például a Twitterhez érkező összesen 5925 kérelemből, mely valamelyik poszt eltávolítására irányult, 3067 származott a török hatóságoktól. A Facebookon 2016 júliusa és decembere között 1111 tartalom törlését érték el. Ankara mindemellett kísérletet tesz az internetes tartalom „manipulálására" is. A hírek szerint egy körülbelül 6 ezer fős „trollhadsereget" tartanak fenn.[30]

Végezetül a Freedom House jelentése a „felhasználói jogok megsértése" területén 40-ből 30 pontra értékelte Törökországot. Online tevékenysége alapján számos embert vettek őrizetbe, általában az elnök megsértésének vagy terrorista propaganda terjesztésének vádja miatt. Arra, hogy a nemzetközi közösség részéről érkező aggályoknak van alapja, jó példa a ByLock nevű telefonos üzenetküldő alkalmazás esete. A 2016. júliusi puccskísérletet követően a letartóztatások alapjául, terhelő bizonyítékként szolgált pusztán az, ha valakinek a telefonján megtalálták az alkalmazást, amit a gyanú szerint egymás közötti kommunikációjuk során a puccsisták használtak. A probléma az, hogy a ByLock egy 41 országban elérhető, népszerű, az Apple és Google áruházakból ingyenesen letölthető alkalmazás volt.[31] Két további példát kiemelve, a nemzetközi médiában is nagy visszhangot kapott, hogy a török hatóságok elítéltek egy korábbi török szépségkirálynőt, Merve Büyüksaraçot az elnök megsértéséért. Büyüksaraç bűne az volt, hogy megosztott a saját Instagramján az egyik újságban megjelent szatirikus költeményt.[32] A török belügyminisztérium közleménye szerint Törökország 2018. januári szíriai katonai beavatkozásának (Olajág hadművelet) kezdetét követően pedig két hét alatt 449 embert vettek őrizetbe a közösségi médiában való terrorista propaganda terjesztésének vádjával, köztük a Török Orvosszövetség 11 tagját, akik háború helyett békére szólítottak fel. Erdoğan árulóknak nevezte a testületet.[33]

ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

Az elmúlt években felértékelődött a kiberbiztonság szerepe a török biztonságfelfogásban. Ezt bizonyítja a folyamatosan fejlődő intézményrendszer és a két elfogadott kiberstratégia. Az okok között az általános világpolitikai trend és a külpolitikai feszültségek mellett meghatározó szerepet játszottak a török belpolitikai fejlemények is.

A kiberbiztonsági eszköz- és szervezetrendszer fejlődése a jelenlegi török belpolitikai és jogi környezetben (tekintetbe véve azt is, hogy a legtöbb törökországi kibertámadás hacktivista támadás, azaz politikailag motivált) a kiberterroristák helyett, illetve mellett az állampolgárokkal szembeni hatékonyabb fellépéshez és szigorúbb korlátozásokhoz vezetett. Megfelelő jogállami garanciák hiányában az állam kibervédelmi képességeinek fejlesz-

[30] Uo.
[31] Uo.
[32] Former Miss Turkey found guilty of insulting Erdogan, 2016. 06. 01. aljazeera.com (A letöltés dátuma: 2018. 05. 07.)
[33] Tuvan Gumrukcu, Dominic Evans: Turkey detains nearly 600 for opposing Syrian offensive, 2018. 02. 05. Forrás: reuters.com com (A letöltés dátuma: 2018. 05. 07.)

tése az autoriter politikai rendszerekben lehetőséget ad arra, hogy egy alapvetően legitim cél (kiberterrorizmus, kiberbűnözés elleni védelem) elérése mellett megkönnyítse a rezsim számára a politikai ellenvélemények elhallgattatását. A törökországi médiaszerkezetet (értsd a törökországi médiumok döntő részének kormányközeli kezekben összpontosulása)[34] és a médiát érintő egyéb korlátozásokat[35] is figyelembe véve a jelenlegi gyakorlat elősegíti a politikai hatalomnak azt a célját, hogy Törökország-szerte egyetlen narratíva érvényesüljön, mégpedig a hivatalos kormányzati narratíva.

FELHASZNÁLT IRODALOM

1. Anonymous - Message to Turkey [Those who support ISIS], 2015. 12. 23. youtube.com (A letöltés dátuma: 2018. 05. 07.)
2. Salih Bıçakcı, Doruk Ergun, Mitat Çelikpala: The Cyber Security Scene in Turkey. In: Sinan Ülgen, Grace Kim (szerk.): A primer on cyber security in Turkey: and the case of nuclear power. 2015, 22–51.
3. Chris Bing: Why Turkey, a NATO ally, is a huge target for malware, 2017. 02. 03. cyberscoop.com (A letöltés dátuma: 2018. 05. 07.)
4. Cyberattacks against Turkey increase sharply, 2017. 12. 02. trtworld.com (A letöltés dátuma: 2018. 05. 07.)
5. ECHR (2016): European Court of Human Rights Judgment in the Case of Artun and Güvener v. Turkey. aihmiz.org.tr (A letöltés dátuma: 2018. 04. 12.)
6. Former Miss Turkey found guilty of insulting Erdogan, 2016. 06. 01. aljazeera.com (A letöltés dátuma: 2018. 05. 07.)
7. Freedom on the Net 2017, Turkey. Freedom House, 2017. freedomhouse.org (A letöltés dátuma: 2018. 05. 07.)
8. Tuvan Gumrukcu, Dominic Evans: Turkey detains nearly 600 for opposing Syrian offensive, 2018. 02. 05. reuters.com com (A letöltés dátuma: 2018. 05. 07.)
9. Internet Users by Country (2016). internetlivestats.com (A letöltés dátuma: 2018. 05. 07.)
10. Major cyber-attack on Turkish Energy Ministry claimed, 2016. 12. 31. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
11. Media Ownership Monitor. turkey.mom-rsf.org (A letöltés dátuma: 2018. 05. 07.)
12. Jason Murdock: Anonymous: Hacker unleashes 17.8GB trove of data from a Turkish national police server, 2016. 02. 16. ibtimes.co.uk (A letöltés dátuma: 2018. 05. 07.)
13. National Cyber Security Strategy 2016–2019. udhb.gov.tr (A letöltés dátuma: 2018. 05. 07.)
14. National Cyber Security Strategy and 2013-2014 Action Plan. enisa.europa.eu (A letöltés dátuma: 2018. 05. 07.)

[34] Az RSF és a Bianet által összeállított Media Ownership Monitor szemléletesen levezeti a tulajdonosi helyzetet. Forrás: turkey.mom-rsf.org (A letöltés dátuma: 2018. 05. 07.)
[35] Lásd például a terrorcselekményekről való tudósítás korlátait. Turkey's TV watchdog introduces new measures limiting terror attacks broadcasting, 2017. 02. 02. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)

15. RedHack discloses IDs of foreign diplomats in Turkey, 2012. 07. 03. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
16. Ahmet Sabanci: Did a single hacker − not Anonymous − cripple Turkey's Internet?, 2015. 12. 28. dailydot.com (A letöltés dátuma: 2018. 05. 08.)
17. Bariş Şimşek (2017): Turkey to prop up cyber defense with new law. dailysabah.com (A letöltés dátuma: 2018. 05. 07.)
18. Terörle Mücadele Kanunu, 1991. mevzuat.tr (A letöltés dátuma: 2018. 05. 07.)
19. Turkey ninth most targeted by cyberattacks, 2016. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
20. Turkey Purge. turkeypurge.com (A letöltés dátuma: 2018. 04. 02.)
21. Turkey shuts down telecommunication body amid post-coup attempt measures, 2016. 08. 17. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
22. Turkey's TV watchdog introduces new measures limiting terror attacks broadcasting, 2017. 02. 02. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
23. Turkey under cyberattack by Russia: Report, 2015. 12. 17. hurriyetdailynews.com (A letöltés dátuma: 2018. 05. 07.)
24. Turkish hackers break into Russian minister's Instagram account, 2016. 01. 03. hurriyetdaily-news.com (A letöltés dátuma: 2018. 05. 07.)
25. Q4 2017 State of the Internet Security Report. akamai.com (A letöltés dátuma: 2018. 05. 07.)
26. Zone-H: http://www.zone-h.org/