Stratégiai Védelmi Kutatóközpont
ELEMZÉSEK 2018/13.

2018. július 11.

Pénzváltó Nikolett:[1] Kiberbiztonság *versus* internetszabadság Törökországban

Vezetői összefoglaló

- Az utóbbi években felértékelődött a kiberbiztonság szerepe Törökországban: egyidejűleg láthatjuk sebezhetőségek jelenlétét és a kibertér aktív (támadó, károkozó célú) felhasználását állami és nem állami szervezetek részéről.
- A 2013-as Nemzeti Kiberbiztonsági Stratégia után 2016-ban újabb stratégiát fogadtak el.
- A geopolitikai és geostratégiai feszültségek középpontjában álló NATO-tag Törökország kiberbiztonsági helyzetének ismerete, valamint a külső támadásokkal szembeni védekező képességének javítása a szövetség számára is kiemelt jelentőséggel bír.
- A kiberbiztonsági eszköz- és szervezetrendszer fejlődése a jelenlegi, rendkívül biztonságiasított török belpolitikai és jogi környezetben a kiberbűnözők és -terroristák helyett, illetve mellett az állampolgárokkal szembeni hatékonyabb fellépéshez és szigorúbb korlátozásokhoz vezetett.
- Megfelelő jogállami garanciák hiányában az állam kibervédelmi képességeinek fejlesztése − a médiát érintő egyéb korlátozásokkal kiegészítve − megkönnyíti a kormányzat számára a politikai ellenvélemények elhallgattatását; ezáltal a hivatalos kormányzati narratíva egyedüliként való érvényesülését segíti elő Törökországban.

Az elmúlt években felértékelődött a kiberbiztonság szerepe a török biztonságfelfogásban (is). Okai között az általános információtechnológiai trend mellett szerepet játszottak a török belpolitikai fejlemények, valamint a politikai–társadalmi feszültség növekedése Törökország közvetlen földrajzi környezetében. A török kiberbiztonsági intézményrendszer folyamatos fejlődése mellett ezt támasztja alá az is, hogy bár a törököknél a stratégiák készítése és publikálása inkább tekinthető esetlegesnek, semmint rendszeresnek,[2] mégis 2016-ban már a második kiberbiztonsági stratégiát fogadták el, amit a török mellett angol nyelven is nyilvánosságra hoztak.

Jelen tanulmány célja kettős: egyrészt áttekintést kíván nyújtani Törökország biztonságának kiberszektoráról; másrészt, rá kíván mutatni azokra a morális aggályokra ezzel összefüggésben, amelyek a jelenlegi, rendkívüli mértékben biztonságiasított török politikai környezet jellegéből fakadnak.

A NATO-tag Törökország geopolitikai és geostratégiai feszültségek középpontjában áll.[3] A szövetség számára ezért is kiemelten fontos a törökországi kiberviszonyok ismerete, különösen miután 2014-ben a kiemelkedően nagy károkozással járó kibertámadások bekerültek a washingtoni szerződés kollektív védelmet biztosító 5. cikkelyének hatálya alá.

Törökország és a kiberbiztonság

Törökország 2016-ban 46 millió fővel a 14. legtöbb internetfelhasználóval rendelkező állam volt a világ országai között.[4] Az internet-penetráció tekintetében azonban nincs ilyen kiemelkedő helyzet: a lakosság mindössze 58%-a rendelkezett internethozzáféréssel.[5] Az információbiztonsággal foglalkozó elemzők adatai szerint nemzetközileg Törökország a kibertámadásoknak egyik leginkább

[1] Pénzváltó Nikolett (penzvalto.nikolett@uni-nke.hu) az NKE SVKK kutatóasszisztense.
[2] Ez alatt azt értjük, hogy nincsenek rendszeres időközönként megjelenő nemzeti biztonsági/védelmi/katonai/egyéb ágazati stratégiák, leszámítva a török Nemzetbiztonsági Tanács által kidolgozott Nemzeti Biztonságpolitika Dokumentumot, az úgynevezett „Vörös Könyvet" (*Kırmızı Kitap*), ami azonban nem nyilvános.
[3] 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 kiberincidensre is sor került. 2016. december 7-én egy órás, úgynevezett szolgáltatásmegtagadással, avagy túlterheléses járó (*Denial of Service* – DoS) 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, [online], 2016. 01. 03. Forrás: hurriyetdailynews.com [2018. 05. 07.]
[4] Internet Users by Country (2016), [online], 2016. Forrás: internetlivestats.com [2018. 05. 07.]
[5] Uo.

kitett országnak számít. Az amerikai FireEye kimutatása alapján 2016-ban Törökországban több célzott malware-támadást észleltek, mint egész Európában összesen.[6] Az STM (*Savunma Teknolojileri Mühendislik ve Ticaret* A. Ş.) információbiztonsági cég 2016-os jelentése a 9. helyre rangsorolta az országot a legtöbb kibertámadást elszenvedő országok listáján.[7] A *Daily Sabah* török napilap szerint Törökország 2017-ben 90 millió kibertámadást szenvedett el. A cikk kiemeli, hogy a támadások száma a 2016 júliusi törökországi puccskísérlet után megsokszorozódott.[8] Kormányzati tisztviselők szerint pedig Törökország az Egyesült Államok és Brazília után a világon a harmadik, támadásoknak leginkább kitett ország, évi közel 25 millió kibertámadással.[9]

Ugyanakkor az Akamai informatikai cég értékelése szerint 2016 első negyedévében – Kína és az Egyesült Államok után –, majd 2017 második negyedévében is – ezúttal Egyiptom és az Egyesült Államok után – Törökország volt a túlterheléses (DDos) támadások harmadik leggyakoribb forrása.[10] Így az országgal nemcsak a támadások célpontjaként, hanem forrásaként is számolnunk érdemes, ami egyidejűleg mutatja sebezhetőségek jelenlétét és a kibertér aktív (támadó, károkozó célú) felhasználását.

Az elmúlt évek nagyobb kibertámadásai török célok ellen

Az elmúlt években Törökországot számos jelentős kibertámadás érte. 2012 júliusában például a Török Külügyminisztérium honlapját törte fel politikai indíttatásból a kormányellenes RedHack Csoport. A támadás során 65 gigabájtnyi belső fájlt szereztek meg, illetve a török külügyi hatóságok által külföldi diplomatáknak kiadott személyazonosító igazolványok adatait szivárogtatták ki.[11] 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.[12] 2016 decemberében pedig a török energiaügyi minisztérium egyik munkatársa magyarázta külső támadással az isztambuli áramkimaradásokat.[13]

Az eddigi legjelentősebb támadásra 2015 decemberében került sor. Az Anonymus hacker-csoport[14] által felvállalt támadás indítékaként az a vád szolgált, miszerint Törökország a kőolaj-vásárláson keresztül, valamint fegyverekkel támogatja az „Iszlám Államot" a szíriai harcokban. A török médiában megjelent spekulációk az oroszokat gyanították a támadás mögött.[15] A tíz napon keresztül tartó túlterheléses 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.[16]

Törökország, mint a kibertámadások forrása – hacktivista és hackercsoportok

Törökországban több jelentős hacker-, illetve hacktivista csoportok tevékenykedik – némelyik kormánykritikus, míg mások nacionalista ideológia mentén akár nyíltan is együttműködnek a kormányzattal és külpolitikai ellenfelek célpontjait (is) támadják.

---

[6] Chris BING: Why Turkey, a NATO ally, is a huge target for malware, [online], 2017. 02. 03. Forrás: cyberscoop.com [2018. 05. 07.]
[7] Turkey ninth most targeted by cyberattacks, [online], 2016. 02. 08. Forrás: hurriyetdailynews.com [2018. 05. 07.]
[8] Barış ŞIMŞEK: Turkey to prop up cyber defense with new law, [online], 2017. 07. 06. Forrás: dailysabah.com [2018. 05. 07.]
[9] Cyberattacks against Turkey increase sharply, [online], 2017. 12. 02. Forrás: trtworld.com [2018. 05. 07.]
[10] Q1 2016 State of the Internet / Security Report, [online], 2016. 21. o.; Q2 2017 State of the Internet / Security Report, [online], 2017. 9. o. Forrás: akamai.com [2018. 05. 07.]
[11] RedHack discloses IDs of foreign diplomats in Turkey, [online], 2012. 07. 03. Forrás: hurriyetdailynews.com [2018. 05. 07.]
[12] Jason MURDOCK: Anonymous: Hacker unleashes 17.8GB trove of data from a Turkish national police server, [online], 2016. 02. 16. Forrás: ibtimes.co.uk [2018. 05. 07.]
[13] Major cyber-attack on Turkish Energy Ministry claimed, [online], 2016. 12. 31. Forrás: hurriyetdailynews.com [2018. 05. 07.]
[14] Anonymous - Message to Turkey [Those who support ISIS], [online], 2015. 12. 23. Forrás: youtube.com [2018. 05. 07.]
[15] Lásd például Turkey under cyberattack by Russia: Report, [online], 2015. 12. 17. Forrás: hurriyetdailynews.com [2018. 05. 07.]
[16] Ahmet SABANCI: Did a single hacker − not Anonymous − cripple Turkey's Internet?, [online], 2015. 12. 28. Forrás: dailydot.com [2018. 05. 08.]

- A *RedHack* csoport küldetésnyilatkozata szerint céljuk egy egyenlő, igazságos és kizsákmányolástól mentes világ megteremtésének támogatása. 2012-2013-ban deface támadást[17] hajtottak végre számos állami szerv weboldala ellen; emellett főként adatszivárogtatások jellemzik a tevékenységüket.
- A *B3yaz Hacker* nevű szerveződés tevékenysége két csoportra osztható: egyrészt sebezhetőségi teszteket (*penetration test*) végeznek, másrészt értékeikkel ellentétes tartalmú oldalakat támadnak.[18]
- A *Turk Hack Team* az egyik legismertebb és legjobban szervezett hacktivista társaság. Önmeghatározásuk szerint tagjaik „a török nemzetért dolgoznak".[19] Jelentősebb támadásaik között említhető a *The New York Times*, illetve a *The Guardian* honlapja elleni akciók, 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; ugyanakkor hajtottak már végre támadást többek között izraeli, örmény, egyiptomi és osztrák célpontok ellen.
- Végül érdemes megemlítenünk a Kurdisztáni Munkáspárthoz (PKK) köthető *PKK Hack Team*et, akikhez a Zone-H weboldal 279 deface támadást köt.[20]

A 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 Teknolojileri ve İletişim Kurumu*, a továbbiakban BTK), amely olyan feladatokat lát el, mint az engedélyezés, felügyelet, fogyasztói jogok védelme, versenyszabályozás, technikai előírások kialakítása, vagy a rádiófrekvenciák használatának szabályozása.[21] A 2016. júliusi törökországi puccskísérletet követő („gülenista" vádak miatti)[22] megszüntetéséig a telekommunikációs eszközökön keresztül zajló 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:[23] természeti és technológiai katasztrófákat) az AFAD a fő koordináló szerv, ami közvetlenül a miniszterelnök irányítása alatt áll. Ki kell emelnünk továbbá az állandó készenlétben működő török incidens-kezelő szervezet (*Computer Emergency Response Team* – TR-CERT)[24] szerepét. A török kiberbiztonsági célkitűzések között szerepel, hogy minden állami intézmény, illetve kritikus

[17] Olyan támadás, melynek során hozzáférnek a célba vett weboldalnak szolgáltatást biztosító szervezhez és megváltoztatják az oldal tartalmát, vagy a teljes felületet egy megváltoztatott megjelenésű, például ellentétes ideológiájú politikai vagy vallási üzenetet hordozó oldalra irányítják át.

[18] A Zone-H összesítése szerint 540 defacement kötődik bizonyíthatóan hozzájuk, főként 2015-ből. Forrás: Zone-H.org [2018. 05. 07.]

[19] A Turk Hack Team honlapja: Misyon (Küldetés), [online], 2018. Forrás: turkhackteam.org [2018. 05. 07.]

[20] Salih BIÇAKCI, 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. o.

[21] BIÇAKCI et. al.: i. m.

[22] Turkey shuts down telecommunication body amid post-coup attempt measures, [online], 2016. 08. 17. Forrás: hurriyetdailynews.com [2018. 05. 07.]

[23] Lásd a 2009. évi 5902. számú törvény definícióit: Afet Ve Acil Durum Yönetimi Başkanliğinin Teşkilat Ve Görevleri Hakkinda Kanun, [online], 2017. Forrás: ecolex.org [2018. 05. 07.]

[24] A Számítógépes Vészhelyzeti Reagáló Csoport / Számítástechnikai Sürgősségi Reagáló Egység, vagy bevett angol rövidítéssel CERT feladata, hogy „hogy időben reagáljon és kezeljen minden hálózatbiztonságra és kritikus információs infrastruktúrára veszélyes internetes eseményt". Kormányzati Eseménykezelő Központ, [online], 2018. Forrás: cert-hungary.hu [2018. 05. 07.]. A török

infrastruktúrát üzemeltető magánvállalat rendelkezzen továbbá saját Szektorális Kiber-incidenskezelő Csapatokkal (*Siber Olaylara Müdahale Ekipleri*, a továbbiakban SOME). A SOME-k működését az TR-CERT, létrehozásukat a Közlekedési, Tengerészeti és Kommunikációs Minisztérium 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.[25]

2012. október 20-án a 2012/3842. számú kormányhatározat (A nemzeti kiberbiztonsági erőfeszítések végrehajtása, menedzselése és koordinálása) hozta létre a Kiberbiztonsági Tanácsot, mely 2013-ban elkészítette az első török Nemzeti Kiberbiztonsági Stratégiát és a kapcsolódó 2013-2014-es Akciótervet. 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 kiberbiztonsági stratégia kiemelt hangsúlyt fektet a kritikus infrastruktúra, a humán tőke és a hazai technológia fejlesztésére. Hiányosságként emeli ki a szakemberek és megfelelő infrastruktúra hiányát, a koordináció hiányát, valamint a törvényi szabályozás elégtelenségét. A dokumentum 29 különálló intézkedési javaslatot sorol fel a kiberbiztonság terén, melyek között szerepel például K+F laborok létrehozása az egyetemeken; egy olyan teszt-infrastruktúra kifejlesztése és telepítése, amely a kulcsfontosságú állami szervezetek adatvesztésének felderítésére szolgál; illetve a Török Nyelvi Szövetség megbízása egy kiberbiztonsági fogalmakat tartalmazó szótár összeállításával.[26]

A 2013-ast követő, 2016-ban elfogadott, 2019-ig hatályos Nemzeti Kiberbiztonsági Stratégia felépítését tekintve négy fő részre tagolódik: 1. Bevezetés, 2. Elvek, 3. Kiberbiztonsági kockázatok, 4. Stratégiai kiberbiztonsági célkitűzések és intézkedések. A dokumentum alkotói felismerték, hogy az abszolút kiberbiztonság napjainkban már nem elérhető, ezért ehelyett a kiberbiztonsági kockázatok kezelhető és elfogadható szinten tartását jelölték meg célként. 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 országokban. E megállapításra hivatkozva, illetve tekintettel elemzésünk fókuszára, a következő alfejezet 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 megszüntetését.[27]

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, hogy hogyan lehet hatékonyan fellépni a támadók ellen úgy, hogy közben ne korlátozzuk a szükségesnél jobban az internethasználó állampolgárok jogait? Kérdéseket vet fel az is, hogy hol húzódik a határvonal a hacktivizmus (politikai aktivizmus a kibertérben) 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 fontosságát, 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 Köztársaságnak az alkotmányban meghatározott (politikai, jogi, társadalmi, gazdasági és szekuláris) jellegének megváltoztatása, az állam oszthatatlan (területi, nemzeti) egységének megkárosítása, az államhatalom meggyengítése vagy a megragadására tett kísérlet. Külön szabályozás vonatkozik a terrorizmus támogatóira. Az egyik leggyakoribb állampolgárokat érő vád a hatalom részéről ezen összefüggésben a szintén tágan értel-

CERT-et (TR-CERT) a török dokumentumok gyakran török rövidítésén, USOM-ként említik (*Ulusal Siber Olaylara Müdahale Merkezi*).

[25] BIÇAKCI et. al.: i. m.

[26] National Cyber Security Strategy and 2013-2014 Action Plan, [online], 2018. Forrás: enisa.europa.eu [2018. 05. 07.]

[27] National Cyber Security Strategy 2016–2019, [online], 2017. Forrás: udhb.gov.tr [2018. 05. 07.]

mezett „terrorizmus párti propaganda folytatása”.[28] Törökország valóban sokat szenvedett a terrorizmustól az utóbbi években: a *Global Terrorism Database* adatai szerint csak 2016-ban 540 terrormerényletben 1004 ember halt meg.[29] A 2016. júliusi törökországi puccskísérletet követően megkezdődött letartóztatási hullám volumene azonban 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.[30] A török politikai–jogi környezet felvázolásakor még egy jogszabályt mindenképpen ki kell emelnünk: akár négy éves 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.[31]

A *Freedom House* 2017-es *Freedom on the Net* című – az internetszabadsággal foglalkozó – jelentése Törökországot a „nem szabad” kategóriába sorolja. A jelentés a hozzáférés, a tartalomkorlátozás és a felhasználói jogok szempontjából értékeli az egyes államokat.[32]

A török hatóságok hatékonyan alkalmazzák eszközként az internethez, illetve bizonyos szolgáltatókhoz, tartalmakhoz való hozzáférés akadályozását. Az egyes korlátozások bevezetésének időzítéséből szintén 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 polgármestert 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 megakadályozzák, illetve késleltessék a rendőri fellépésekről 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 „szabadnak”.[33]

A „tartalomkorlátozás” területén 35-ből 23 pontra értékelték a törökországi 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 a terrortámadásokat, letartóztatásokat követő tiltó kormányzati lépésekhez. Az internetes tartalmak szabad elérésének további akadályozása érdekében 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 második felében például a Twitterhez érkező összesen 5 925 kérelemből, amely valamelyik poszt eltávolítására irányult, 3 067 származott a török hatóságoktól. A Facebookon 2016 júliusa és decembere között 1 111 tartalom törlését érték el. Ankara mindemellett kísérletet tesz az internetes tartalom „manipulálására” is. E célból a hírek szerint egy körülbelül 6 ezer fős „trollhadsereget” tartanak fenn a hatóságok.[34]

Végezetül a *Freedom House* jelentése a „felhasználói jogok megsértése” területén 40-ből 30 pontra értékelte Törökországot. Online tevékenysége miatt számos embert vettek őrizetbe, általában az elnök megsértésének vagy terrorista propaganda terjesztésének vádjával. 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.[35] 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

[28] A jogszabály szövege török nyelven: Terörle Mücadele Kanunu, 1991, [online], 2017. Forrás: mevzuat.tr [2018. 05. 07.]
[29] Ez a szám tartalmazza a júliusi puccskísérletben életüket vesztettek számát is.
[30] Turkey Purge, [online], 2018. Forrás: turkeypurge.com [2018. 05. 02.]
[31] ECHR (2016): European Court of Human Rights Judgment in the Case of Artun and Güvener v. Turkey, [online], 2017. Forrás: aihmiz.org.tr [2018. 04. 12.]
[32] Freedom on the Net 2017, Turkey, [online], 2017. Forrás: freedomhouse.org [2018. 05. 07.]
[33] Uo.
[34] Uo.
[35] Uo.

egy, az egyik újságban megjelent szatirikus költeményt.[36] 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 szervezetet.[37]

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 technológiai 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 fejlesztése 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 (a törökországi médiumok döntő részének kormányközeli kezekben összpontosulását)[38] és a médiát érintő egyéb korlátozásokat[39] is figyelembe véve a jelenlegi gyakorlat elősegíti a politikai hatalomnak azt a célját, hogy Törökországszerte egyetlen narratíva érvényesüljön, mégpedig a hivatalos kormányzati narratíva.

[36] Former Miss Turkey found guilty of insulting Erdogan, [online], 2016. 06. 01. Forrás: aljazeera.com [2018. 05. 07.]
[37] Tuvan GUMRUKCU, Dominic EVANS: Turkey detains nearly 600 for opposing Syrian offensive, [online], 2018. 02. 05. Forrás: reuters.com com [2018. 05. 07.]
[38] Az RSF és a Bianet által összeállított Media Ownership Monitor szemléletesen levezeti a tulajdonosi helyzetet. Forrás: turkey.mom-rsf.org [2018. 05. 07.]
[39] Lásd például a terrorcselekményekről való tudósítás korlátait. Turkey's TV watchdog introduces new measures limiting terror attacks broadcasting, [online], 2017. 02. 02. Forrás: hurriyetdailynews.com [2018. 05. 07.]

Az „SVKK Elemzések” 2003 óta a Kutatóközpont munkatársainak tematikus szakpolitikai elemzéseit megjelentető időszakos kiadvány, melyben a szerzők független kutatói álláspontjukat közlik.

Kiadó: Nemzeti Közszolgálati Egyetem

Szerkesztés és tördelés:
Bazsó Márton, Csiki Tamás

A kiadó elérhetősége:

1581 Budapest, Pf. 15.

Tel: 00 36 1 432-90-92

E-mail: svkk@uni-nke.hu

2012– : NKE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4862)

2011–2012: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)
2007–2011: ZMNE Stratégiai Védelmi Kutatóintézet Elemzések (ISSN 2063-4854)
2003–2007: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)