

CSEGE Gyula

PhD-hallgató

Pécsi Tudományegyetem Földtudományok Doktori Iskola

PhD student

**University of Pécs Faculty of Science Doctoral School of Earth Sciences,
Pécs, Hungary**

gyulacsege@gmail.com

RENDESZETI SZERVEK A BIZTONSÁGI KIHÍVÁSOKKAL ÖSSZEFÜGGÉSBEN, AZ INFORMÁCIÓÁRAMLÁS TÜKRÉBEN

*POLICE ORGANISM AND SAFETY CHALLENGES, IN MIRROR
OF INFORMATION FLOW*

ABSTRACT

In recent decades, policing has undergone major changes, with changes and expansion of the private sector and social needs, the reorganization of national security services and law enforcement agencies to a large extent affecting security levels.

My goal is to present the actors of private security and national security and the needs caused by social and security challenges, along with the security phenomena that accompany our day, such as change in law enforcement, terrorism, migration, and certain aspects of cyberspace in relation to information flow issues.

Kulcsszavak: rendészeti szervek, biztonsági kihívások, információáramlás

Keynotes: police organism, safety challenges, information flow

1. Bevezetés

A közelmúlt, illetve a jelen idők tapasztalatai és ez irányú kutatásai egyértelműen bizonyították, hogy a biztonsági és geopolitikai tekintetben is meghatározó kockázatok jelentős része, mint a szervezett bűnözés, az extrémizmusok, valamint a terrorizmussal kapcsolatba hozható személyek és csoportok kapcsolattartása, koordinációja és népszerűsítési iránya az internet használata felé tolódik, és vezető szerepre is az online csatornákon törekszik.¹

A kapcsolattartási metódusok mellett a tartalmak megosztása, adatbázisok használatának megváltozása során számos új tendencia mérhető, amelyre az elmúlt évek megemelkedett biztonsági kockázataival szembenező államoknak is válaszolniuk kell.²

A helyes és hatékony reakcióhoz és a felkészülés szükségességéhez át kell tekintenünk, milyen kérdések adódhatnak a vizsgált területtel kapcsolatban, hogyan állapítható meg, jelenleg milyen feladatok valósultak meg, és melyek azok a megnyugtató intézkedések, amelyekkel megállítható, korlátozható, illetve ellenőrizhető az online térben megosztott adatok segítségével folytatott támadásokra történő felkészülés, vagy a szélsőséges kommunikáció, továbbá a terrorcsoportok propagandája.³ Meg kell állapítanunk, melyek azok a felületek, melyek a biztonsági kockázatokkal kapcsolatos népszerűsítő weboldalak, amelyeken szükséges ellenőriznünk a videók, képanyagok, dokumentációk megosztását.⁴

Hogyan ellenőrizhetőek ezek a csatornák, miként lehet megállapítani, kik regisztráltak ezekre a felületekre, milyen lehetőség van az adatforgalom ez irányú monitorozására, milyen bűncselekményt követ el az, aki az interneten szándékozik szervezett bűnözői csoportokat fenntartani vagy támogatni, népszerűsíteni a szélsőséges ideológiákat, milyen oldalak és fórumok jelentek meg a korábbi elkövetett cselekményeknél.⁵ Hogyan lehet felkészülni a témához kapcsolódó kockázatokra, melyek azok a jogszabályi keretek, amelyek lehetőséget adnak ennek ellenőrzésére, hol végződik a magánszféra ebben az esetben, valamint meddig tart a jogszabályi védelem.

2. Napjainkban

A kockázatok felmérése érdekében szükséges vizsgálnunk a hazai képességeket, azt, milyen rendvédelmi szervek foglalkoznak-foglalkozhatnak jogszerűen a biztonsági kockázatok vizsgálatával a kibertér tartalmak monitorozásával.

A nemzetbiztonsági törvény⁶ alapján elektronikus tartalmak ellenőrzését jogszerű céllal és engedéllyel a nemzetbiztonsági kockázatok felderítése céljából az Alkotmányvédelmi hivatal, az Információs Hivatal, a Katonai Nemzetbiztonsági Szolgálat, a Terrorellhárítási Információs és Bűnügyi Elemző Központ, a Nemzetbiztonsági Szakszolgálat, valamint a Terrorellhárítási Központ végezheti. A felsorolt szervek egyike sem nyomozó hatóság. Az ellenőrzés és az információ ebben a kérdéskörben nem minden esetben elégséges, ameddig nem tudjuk ezt megnyugtatóan feldolgozni, és az érintetteket bíróság elé állítani, meggátolni bűnözők kommunikációját, a szélsőséges ideológiák terjesztését, addig nem lehet megfelelő választ kiala-

kítani a felvetődő kockázatokra. A két területet azonban el kell választani egymástól. A kockázatok⁷ felmérése során más körülmények igazolásának szüksége, mint egy nyílt büntetőeljárás⁸ folyamán.

Fontos még a kérdéskör, és vizsgálatra szorul, hogy milyen változások szükségesek ennek ellenőrzésében annak megállapítására, hogyan hozhatók nyilvánosságra⁹ a kockázatosnak ítélt információk, hogyan lehet azokat a weboldalakot feltérképezni, amelyek külföldi szerverekről működnek, hogyan lehet ezek tartalmát megváltoztatni, vagy egyenesen hozzáférhetetlenné tenni. Ennél a kérdésnél a sajtóból is ismert Kuruc.info oldallal kapcsolatos intézkedések és lehetőségek nyújthatnak támpontot.¹⁰

A szervezett bűnözéssel, valamint a szélsőséges tevékenységgel, terrorizmussal kapcsolatos területen formálisan van nemzetközi együttműködés titkosszolgálati, rendvédelmi szinten, de gyakorlati megvalósulása az Európai Unió Biztonságtudományok Intézete vizsgálata alapján akadályokba ütközhet.¹¹

3. Hatáskör és illetékesség

A kérdést a vizsgált terület komplexitása tükrében első körben nemzeti titkosszolgálati szinten kell megközelíteni, az adatgyűjtést az erre jogosult szervek el tudják végezni jogszabályi lehetőségeik és technikai feltételeik alapján.

A jogszabályi felhatalmazás vizsgálatából kiindulva a nemzetbiztonsági törvény 5. §-a szerint az Alkotmányvédelmi Hivatal feladata Magyarország alkotmányos rendjének törvénytelen eszközökkel történő megváltoztatására vagy megzavarására irányuló leplezett törekvések felderítése és elhárítása.

Az alkotmányos rendet több irányból érhetik támadások, az annak megváltoztatására vagy megzavarására irányuló leplezett törekvések különböző formában és intenzitással jelentkezhetnek. Az alkotmányos rendet éppúgy veszélyeztethetik a szélsőséges vallási törekvések, mint a demokratikus jogrendet elutasító ideológiai alapon szerveződő, vagy erőszak alkalmazására kész csoportok. Az alkotmányos garanciák fenntartása fontos összetársadalmi érdek, így a jogalkotó az Alkotmányvédelmi Hivatal velük kapcsolatos információgyűjtő tevékenységéhez – a törvényben rögzített feltételek fennállása esetén – a titkosszolgálati eszközök és módszerek¹² alkalmazását is lehetővé tette.¹³

Az Információs Hivatal aktív szerepet vállal a terrorizmus elleni küzdelemre irányuló titkosszolgálati együttműködésben, amely során Magyarország részt vesz a szervezett bűnözéssel kapcsolatos, valamint a nemzetközi terrorizmus kockázatainak közös elemzésére, értékelésére és

kezelésére szolgáló különféle nemzetközi kezdeményezésekben. A nemzetközi szervezett bűnözés és a terrorizmus elleni küzdelem összkormányzati tevékenység, amelyen belül az Információs Hivatal Magyarország biztonságát, politikai, gazdasági és más érdekeit, állampolgárait veszélyeztető, ideológiailag motivált, politikai célokat követő nemzetközi bűn és terrorszervezetek és külföldi szélsőséges csoportok struktúrájára, tagjaira, tervezett erőszakos cselekményeire, támogatói körére, pénzügyi-gazdasági hátterére és infrastruktúrájára vonatkozó, a terrorcselekmények megelőzését célzó titkosszolgálati tevékenységet folytat. Az állami-politikai döntéshozók tájékoztatása érdekében figyelemmel kíséri az egyes államok és a nemzetközi szervezett bűnözés és a terrorszervezetek közötti összefonódásokat, a titkosszolgálatok és a terrorista szervezetek, szélsőséges politikai-vallási csoportok közötti kapcsolatokat, a terrorista szervezetek által alkalmazott új módszereket (például internet-használat), a terrorszervezetek biológiai, illetve vegyi fegyverek előállítására vonatkozó törekvéseit.¹⁴

A Terrorelhárítási Központ szintén igen jelentős részben képes hozzájárulni anyagi, technikai és személyi lehetőségeihez mérten a szélsőséges ideológiák interneten történő információ és adatcserék segítségével történő terjedésének feltérképezéséhez, valamint a szervezett bűnözői csoportok és terrorszervezetek kommunikációjának, propagandájának felderítéséhez.¹⁵ A Terrorelhárítási Központnak nincs titkosszolgálati és nyomozati jogköre, azonban a rendőrség terrorizmussal kapcsolatos feladatainak ellátására létrehozott önálló költségvetési szerv.¹⁶ A magyarországi terrorfelderítést a rendőrségi törvény egyértelműen szabályozza, az ezzel kapcsolatos jogosítványokkal a rendőrséget ruházza fel.¹⁷

Az említett nemzetbiztonsági szolgálatok és rendőrségi szervek a központi koordinációs feladatokat ellátó szerv, a Terrorelhárítási Információs és Bűnügyi Elemző Központnak jeleznek a nemzetbiztonsági érdeksérelem elkerülése érdekében.¹⁸

A Tibek a megismert információ teljes spektrumára vonatkozó adatokat meg tudja adni a nyomozó hatóságoknak vagy az Európai Unió központi koordinációs bizottságainak, tehát a területen ennek figyelembevételével megvalósuló feladatmegosztást lehet végrehajtani, a jogszabályok adta keretek betartásával. A nyomozó hatóságok a tényleges bűnügyi relevanciánál jelzést kapnak a Tibektől, és így érdemi nyomozást, esetleg operatív nyomozó hatósági felderítést végezhetnek a Magyarországon üzemelő szervezett bűnözők által használt felületek, illetve az extrémizmus-népszerűsítő oldalak, tartalom megosztások kapcsán. Az ilyen jellegű cselekmények nehezen megfogható és értelmezhető vetületei

miatt egy szerv önmagában nem minden esetben képes megnyugtatóan elvégezni azt a feladatot, amit az európai uniós kötelezettség a nemzetközi szervezett bűnözés és az extrémizmus terrorizmussal kapcsolatos feladatként meghatároz.

Fontos továbbá a szervezett bűnözők általi, illetve az extrémizmus-terrorizmus jelenleginél erősebb vetületeivel kapcsolatos megosztási arányok emelkedése. A netes szélsőséges bűnözői és terroristatoborzás és népszerűsítés nemzetbiztonsági kockázatokkal jár, azonban büntetőjogi vetület és büntetőjogi relevancia a hatályos büntető törvénykönyv rendelkezései és a joggyakorlat alapján nehezen mutatható ki.¹⁹ A terrorizmussal kapcsolatos erőszakos bűncselekményeknél árnyaltabb képet mutat a háborús uszítás, amelynél az internetes megosztások, videók, propagandafeltöltések ütköztethetők, a 2012. évi C. törvény, azaz a Büntetőtörvénykönyv 331. § b) pontja alapján, aki nagy nyilvánosság előtt a terrorizmus támogatására uszít, vagy egyébként a terrorizmust támogató hírverést folytat, azokat büntetni rendeli a jogszabály. Szélesebb körű kockázatot jelenthetnek ennek fogadói, vagyis a tartalmak figyelői és nézői, ez a nemzeti információk érdekeken is túlmutathat.

A szervezett bűnözés és a szélsőséges ideológiák biztonsági kérdéseinél meg kell említenünk a fent felsorolt szervek mellett az általános rendőri szerv egy tagját. A készenléti rendőrség Nemzeti Nyomozó Iroda Felderítő Főosztálya a büntetőeljárásról szóló 2017. évi XC. törvény alapján előkészítő eljárás keretein belül felderítheti a nemzetközi szervezett bűnözői körök, a terrorizmussal kapcsolatba hozható internetes tartalmak, vagy más kibertérben zajló folyamatok büntetőjogi relevanciáját, hiszen az egyetlen általános rendőri szerv, amely a jogszabályi környezet vizsgálva kompetens lehet ez irányú felderítésre. Meg kell említenünk, hogy nyílt büntetőeljárások szükségessége esetén át kell adni a nyomozásokat a területileg illetékes nyílt nyomozó szervnek.

4. Geopolitikai, nemzetközi vetületek

Nemzetközi szövetségi rendszerünkben az említett körülményeknek összeurópai, szövetségi érdeket is szolgálniuk kell, e miatt az együttműködés magasabb szintre emelkedett az elmúlt évben a korábbi közös EU politikai munka mellett létrehozásra került az úgynevezett Europol's European Counter Terrorism Centre (ECTC), amelyen belül az EU Internet Referral Unit (IRU). Az ECTC az Europol szervezeti egysége a terrorizmussal kapcsolatos feladatok elvégzésére, amely mellett egy kifejezetten kibertérben elkövetett cselekményekkel összefüggő csoport került kialakításra. Az egység a beszámolója alapján eredményes munkát végez: A

tendenciákat szemléltetve 2015-ös beszámoló alapján 1079 ténylegesen értékelt tartalmat mutató adatot tett közzé, míg 2016. július 1-jén ez az adat már 11 050. Ugyanebben az időszakban az internetről eltávolított anyagok száma 511-ről 8949-re növekedett.²⁰ Az IRU 2017-től saját 24 órás monitorozást és szakmai munkát tervez az egyre több feladat miatt. A felderítés és jelzés exponenciális emelkedést mutat évről évre.²¹

5. Lehetséges nemzeti megoldások

A szükséges lépések között megfontolandó lehet az eredményesebb felderítéshez a polgári titkosszolgálatok és az információ gyűjtő szervezetek részére egy intézkedési terv, amely dinamizálhatja a nyílt nyomozó hatóságokkal kapcsolatos adat és információátadási munkát.²² Ez alapján a kibertérben szervezett bűnözői körökkel kapcsolatos, illetve a szélsőséges ideológiákat terjesztő és megosztó, illetve tartalom használói irányokba magasabb fokú és célirányos adatgyűjtést hajthatnak végre a hatáskörrel rendelkező szervek. A megismert és ekkor már minősített adatokat, a jogi szignalizáció után TIBEK koordináció alapján és az elemzési munkát követően IRU tájékoztatással lehetne megnyugtatóan nemzetközi, tartalomszolgáltatói szinten kezelni, míg nemzeti szinten a nyílt nyomozó szervek egy tagját automatikusan bevonnák a munkába. Ennél a folyamatnál a határidő rövidülésére lehet számítani, mivel esetleg gyorsan eltávolíthatják a vizsgált kiber térben lévő tartalmakat. Nemzeti szinten továbbá a büntető jogszabályi ütköztetéssel nyomozás folytatható, erről az információ súlyossága, relevanciája és érintettség köre alapján dönthet a nemzetbiztonsági törvény alapján a TIBEK. A terület bűnügyi vetületei alapján kijelölt nyomozó hatóság a kérdéskörben a Készenléti Rendőrség Nemzeti Nyomozó Iroda Felderítő Főosztálya, illetve az extrémizmusokkal kapcsolatban felvetődő bűncselekmények alapján más nyomozó hatóságok bevonásával megnyugtatóan kezelhetőek a felmerült adatok az igazságszolgáltatás előtt. A nyomozati szakot szintén adatpontosító céllal megelőzheti az operatív felderítés,²³ amely a nemzetbiztonsági jelzésre reagálva és ezzel összefüggésben képes feltérképezni a szélsőséges ideológiák hazai hirdetői, illetve fogadói csoportjait és érintettjeit. Az új büntetőeljárás törvény alapján azonban egy helyen kell ehhez az előkészítő eljárást és a nyílt nyomozást is lefolytatni, megfelelő szervezeti adottságok mellett.

A vizsgált információknál igen fontos körülmény, hogy önmagában egy rendvédelmi szerv kevés esetben tudja hatékonyan kezelni, teljeskörűen feldolgozni. Az esetek egy részénél központi összefogásra, magas szintű koordinációra és határozott állományilletékes vezetői feladatmeg-

határozásra van szükség, tekintettel arra, hogy az ilyen típusú kibertérhez kapcsolódó kiemelt szervezett bűnözéssel összefüggő, terrorhoz vagy extrémizmushoz kapcsolódó adatok és szélsőséges ideológiákat népszerűsítő és toborzó csatornák is, olyan későbbi veszélyeket rejtenek, olyan eljárásrendeket hoznak a felhasználók körében, amelyek segítségével magasabb fokú terrorirányú szervezkedés valósulhat meg.

A magas szintű információcsere idején sor kerülhet azoknak az adatoknak az elemzésére, hogy ki milyen gyakorisággal használja hazánkban a darkweb²⁴ vagy rejtőzködésre alkalmas csatornákat. Szükséges Magyarországon is egy eljárásrend azoknak a feltérképezésére, akik rendszeres látogatói az ilyesféle oldalaknak, felületeknek, amelyek ismert szervezett bűnözői körökhöz kapcsolhatók vagy terror és szélsőséges ideológiákat népszerűsítő fórumoknak, így e személyek büntetőeljárás alá vonása is megvalósulhat. Nem minden esetben elég az információ, a bűnöző vagy szélsőséges egyének drasztikus elrettentéséhez nyílt lépés is indokoltá válhat, e demonstratív folyamatok elrettentő erőként jelentkezhetnek a szélsőséges folyamatok kialakulásánál.

A nemzeti, illetve az európai szintű együttműködés igen fontos, tekintettel arra, hogy a résztvevők által kijelölt összekötők, a gyakorlati információkat átadók olyan tapasztalatokat gyűjthetnek, illetve olyan felméréseket végezhetnek, amelyek segítségével gyorsan tudnak tendenciákat követni. A felmérések és az összeurópai új irányok megmutathatják, hogy mely országban milyen formában kerül sor tiltott tartalmak feltöltésére, milyen fontos csatornákat használnak az érintettek, milyen biztonsági szoftverek és biztonsági csatornák, illetve titkosítási folyamatok látszanak a háttérben.

6. Összegzés

A vizsgált terület igen fontos, és széles spektrumban értékelhető. A témának biztonságpolitikai, nemzetbiztonsági, nemzetközi, rendvédelmi, informatikai, kiberbiztonsági vetületei is vannak, de ebben az időszakban talán a legfontosabb a kockázatok felmérése, és nemzeti szintű válaszadás. A nemzetközi szinten rendelkezésre álló lehetőségek, mint például az uniós és a rendvédelmi együttműködések igazolják a terület fontosságát és szükségességét.

A kockázatok legfaj súlyosabban az online felületen jelennek meg, a szervezett bűnözői körök tevékenysége, a szélsőséges ideológiák, valamint a terrorizmussal kapcsolatos propaganda terjesztésével. Az intézkedés szükségessége nemzetközi szinten emelkedő tendenciát mutat, de megjelennek azok az információk is, hogy az államok közötti titkosszol-

gálati adatcsere nehézségekbe ütközik. Ez megjelenhet a nemzeti szinten is a jelenlegi struktúrában.

A nehézségek kiküszöbölése igen összetett terület, hiszen minden állam titkosszolgálatát védi a saját forrásait és adatbázisait, mint ahogy azt az Európai Unió erre vonatkozó kutatásai is igazolják.²⁵ A tapasztalatok alapján a nemzet érdeke előrébb való a közös érdeknél, és ez akadályozhatja a hatékony felderítést.

Hazánkban a nemzeti szintű felderítési rendszerben nagy lehetőségei vannak, mivel a titkosszolgálatok és a rendőrség nemzetközi együttműködésben tevékenykedő egységeinél is jelentős szakembergárda dolgozik. A központi koordináló szerv létrehozásával 2016-ban szervezeti változások is történtek a területen, valamint a kibertérrel összefüggő 2017-es K + F kutatások, jelentős rendőri és titkosszolgálat fejlesztések is megvalósultak.²⁶

Azonban jelentős probléma, hogy hatványozottan növekedhetnek a szervezett bűnözéssel és a terrorizmussal kapcsolatba hozható tartalmak, így szükség lesz az említett szervek anyagi, szakmai fejlesztésére.

A másik szükséges fejlesztési terület a propaganda és toborzó tartalmakkal kapcsolatos információk szélesebb körű megosztása, mivel az elkövetés sem nemzeti szinten valósul meg.

A gyors információcserénél talán az egyik legfontosabb szempont a megjelenő hazai szervezett bűnözői és szélsőségestartalom-fogyasztói kör feltérképezése, ezt segíthetik a nemzetközi együttműködésből származó adatok és a hazai felderítés. A visszatérő rejtőzködő bűncselekményre vagy terrorcselekményre használható felületek látogatói, szimpatizánsok feltérképezése csak szoros és gyors nemzetközi szakmai együttműködés mellett valósulhat meg. A biztonságilag kockázatos tartalom-fogyasztói monitorozás hosszú távú eredményekkel járhat, hiszen a felderített veszélyes tartalom felfüggesztése után a vizsgált személy új kockázatos felületeket fog keresni, immár már a hatóságok látókörében.

Az elmúlt években bekövetkezett események és a biztonsági szint növekedése nyomán a szervezett bűnözői körök és a terrorszervezetek, a szélsőséges ideológiák terjesztőinek hírközlési lehetőségei egyre szűkülnek. A zártabb határok és ellenőrzöttebb schengeni zóna²⁷ miatt az online felületre kerülhet az ilyen szervezetek hírközlése is. Fontos kiemelni, hogy az eddig bűnözői körök és a szélsőségesek által használt információs csatornákat a titkosszolgálatok és a nyomozó szervek európai szinten nyilvánvalóan ellenőrzés alatt tartják, így megszűntek azok a biztonságos csatornák, amelyeken az szervezett bűnözői tevékenységben és a terrorizmusban érintett személyek és csoportok kockázatmentesen kommunikálhattak.

A határok lezárásával és erősebb ellenőrzésével a futárok, illetve a közvetlen kapcsolattartásban részt vevők utaztatása nem lehet perspektíva. Az internet azonban kiváló terep az információátadásra és adatcserére, bár ennek ellenőrzése is folyamatos az Európai Unióban, így a bűnözői csoportok és a terrorszervezeteknek olyan fajta információközlési metódusokat kell kidolgozniuk, amellyel nagyon gyorsan és célravezetően juttathatják el az együttműködőknek az információt.

JEGYZETEK/NOTES

1. Gabriel Weimann (2010): Terror on Facebook, Twitter, and Youtube. *The Brown Journal of World Affairs*, vol. 14, iss. 2, pp. 1–3.
2. Gabriel Weimann (2006): Virtual Disputes: The Use of the Internet for Terrorist Debates. *Studies in Conflict and Terrorism*, vol. 29, no. 7, pp. 623–639.
3. Paul Gill (2016): Online Behaviours of Convicted Terrorists. *VOX-Pol Publ.*, p. 4.
4. Amy E. Thornton (2015): Understanding Radicalisation. Doctoral thesis. University College London.
5. Jacob A. Ravndal (2014): The Online Life of a Modern Terrorist: Anders Behring Breivik's use of the Internet. *VOX-Pol*, October 28, 2014. <http://www.voxpol.eu/the-online-life-of-a-modern-terrorist-anders-behring-breiviks-use-of-the-internet/>
6. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.
7. Véletlen, egyedileg nem látható és nem akart jövőbeni esemény lehetősége, amely új szükségletet, kárt, veszteséget, hátrányt, nem kívánatos állapotot okoz. 2. Bizonytalan bekövetkezésű negatívan értékelt következmény. A veszély realizálódásának valószínűsége. Rendészettudományi szöszedet, Magyar Rendészettudományi Társaság, Budapest, 2008
8. A büntetőeljárásról szóló 1998. évi XIX. törvény rendelkezései szerint.
9. A minősített adat védelméről szóló 2009. évi CLV. és a büntetőeljárásról szóló 1998. évi XIX. törvény rendelkezéseinek együtt alkalmazása során.
10. A Kuruc.info weboldal tartalma vonatkozásában a II. és III. Kerületi Ügyészség a honlapon egy 2013 júliusában megjelenő, a holokausztot tagadó megállapításokat tartalmazó cikkének végleges hozzáférhetetlenné tételét kezdeményezte, mivel az írás kétségbe vonja a haláltáborban történő rémtetteket. Ebben az ügyben az eljárásra illetékes Budapest II. és III. Kerületi Bíróság a cikk és az ahhoz fűzött hozzászólások végleges hozzáférhetetlenné tételét rendelte el. 2015 májusában a Budapesti V. és XIII. Kerületi Ügyészség indítványozta a Kuruc.info.hu egyik aloldalának teljes blokkolását, a nemzeti-szocialista rendszerek bűnei nyilvános tagadásának büntette miatt. Az Egyesült Államok egyik szerverén tárolt weboldal adatait a mai napig nem lehetett eltávolítani technikai és jogsegélynehézségek miatt.

11. Björn Fagersten (2016): For EU eyes only? Intelligence and European security. Institute for Security Studies, no. 8. pp. 1–4.
12. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 54. és 56. §-ai alapján.
13. <http://ah.gov.hu/html/alkotmanyvedelem.html>
14. http://www.mkih.hu/feladatok_terrorizmus.shtml
15. A terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) kormányrendelet 2. § (1) bek. A kormány a rendőrségről szóló 1994. évi XXXIV. törvényben meghatározott terrorizmust elhárító szervként a Terrorelhárítási Központot jelöli ki.
16. A rendőrségről szóló 1994. évi XXXIV. törvény 1. § (1) bek. A rendőrség feladata az alaptörvényben meghatározott feladatok mellett a határforgalom ellenőrzése, a terrorizmus elleni küzdelem és az e törvényben meghatározott bűnmegelőzési, bűnfelderítési célú ellenőrzés, valamint a bűncselekményből származó vagyron visszaszerzése.
17. A rendőrségről szóló 1994. évi XXXIV. törvény 10. § Magyarország területén a) felderíti a terrorszervezeteket; b) megelőzi, felderíti, illetve elhárítja magánszemélyek, csoportok, szervezetek terrorcselekmény elkövetésére irányuló törekvéseit és megakadályozza azt, hogy bűncselekményt kövessenek el; c) megakadályozza, hogy magánszemélyek, csoportok, szervezetek terrorszervezet működését anyagi források biztosításával vagy más módon elősegítsék [...]
18. 1995. évi CXXV. törvény 8/A § k) pont: figyelemmel kíséri a bűnszervezetek és terrorszervezetek, valamint a szervezett bűnözői és terrorista csoportok tevékenységét, az ilyen szervezetek és csoportok egymáshoz való viszonyát, kapcsolatait, a jogsértő módon szerzett vagyonuk, illetve az ilyen vagyon jogsértő eredetének leplezésére irányuló törekvéseik és az ilyen célt szolgáló vállalkozásaik elemzésével segítséget nyújt az ellenük való fellépéshez [...]
19. Büntető törvénykönyv 2012. évi C. törvény 314. § b) pont: Aki abból a célból, hogy állami szervet, más államot vagy nemzetközi szervezetet arra kényszerítsen, hogy valamit tegyen, ne tegyen vagy eltűnjön terrorista csoportot szervez. 316. §: Aki a) terrorcselekmény elkövetésével fenyeget; vagy b) terrorista csoporthoz csatlakozás céljából Magyarország területéről kiutazik vagy azon átutazik 318. § (1) bek.: Aki terrorcselekmény feltételeinek biztosításához anyagi eszközt szolgáltat vagy gyűjt, vagy terrorcselekmény elkövetésére készülő személyt vagy rá tekintettel mást anyagi eszközzel támogat, büntett miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő. 331. § (1) bek.: Aki nagy nyilvánosság előtt háborúra uszít, vagy egyébként háborús hírverést folytat, büntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő. (2) bek.: Az (1) bekezdés szerint büntetendő, ha súlyosabb bűncselekmény nem valósul meg, aki nagy nyilvánosság előtt a terrorizmus támogatására uszít, vagy egyébként a terrorizmust támogató hírverést folytat.
20. <https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights>

21. [https://www.europol.europa.eu/publications-documents?y\[value\]\[year\]=2018](https://www.europol.europa.eu/publications-documents?y[value][year]=2018)
22. Az „extrém-terror online protokoll” egyértelműsítene és határidőhöz kötné az internetes feladatokat a rendvédelem teljes spektrumában, valamint egy egyértelmű és objektív „extrém-terror skálán” azonnal jelzéssel elhelyezett észlelésekkel gyorsítani és standardizálni lehetne a területen felvetődő adatokat.
23. A rendőrségről szóló 1994. évi XXXIV. törvény 64. és 69. § rendelkezései szerint.
24. The dark web, also referred to as the darknet, is an encrypted portion of the internet that is not indexed by search engines. The dark web is a subsection of the deep web. / A sötét web, amelyet más néven darknetnek neveznek, az internet titkosított része, amelyet a keresőmotorok nem indexelnek. A sötét háló a mélyháló alszakaszát képezi. <https://whatis.techtarget.com/definition/dark-web>
25. Fagersten, Björn: For EU eyes only? Intelligence and European security. Institute for Security Studies, no. 8.
26. <https://akk.uni-nke.hu/kutatas-tudomanyos-elet/kiberbiztonsagi-akademia/bemutatkozas>
27. A luxemburgi Schengenben 1985. június 14-én aláírt egyezmény, amely szerint a személyazonossági okmányok bemutatása megszűnt mindazok számára, akik az Európai Unió belső határállomásain kelnek át, legyenek akár az unió állampolgárai, akár más ország lakói. Magyarország vonatkozásában 2007. december 21. óta hatályos.

FELHASZNÁLT IRODALOM/REFERENCES

- Fagersten, Björn (2016): For EU eyes only? Intelligence and European security. Institute for Security Studies, no. 8.
- Gill, Paul (2016): Online Behaviours of Convicted Terrorists. VOX-Pol Publ.
- Ravndal, Jacob A. (2014): The Online Life of a Modern Terrorist: Anders Behring Breivik’s use of the Internet. VOX-Pol, October 28, 2014. <http://www.voxpol.eu/the-online-life-of-a-modern-terrorist-anders-behring-breiviks-use-of-the-internet/>
- Thornton, Amy E. (2015): Understanding Radicalisation. Doctoral thesis. University College London.
- Weimann, Gabriel (2006): Virtual Disputes: The Use of the Internet for Terrorist Debates. Studies in Conflict and Terrorism, vol. 29, no. 7.
- Weimann, Gabriel (2010): Terror on Facebook, Twitter, and Youtube. The Brown Journal of World Affairs, vol. 14, iss. 2.

Internetes hivatkozások

- <http://ah.gov.hu/html/alkotmanyvedelem.html> (Letöltve: 2019. 03. 02.)
- http://www.mkih.hu/feladatkorok_terrorizmus.shtml (Letöltve: 2019. 03. 02.)
- <https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights> (Letöltve: 2019. 03. 02.)
- <https://whatis.techtarget.com/definition/dark-web>(Letöltve: 2019. 03. 02.)

[https://www.europol.europa.eu/publications-documents?y\[value\]\[year\]=2018](https://www.europol.europa.eu/publications-documents?y[value][year]=2018)
(Letöltve: 2019. 03. 02.)

<https://akk.uni-nke.hu/kutatas-tudomanyos-elet/kiberbiztonsagi-akademia/bemutakozas> (Letöltve: 2019. 03. 02.)

<http://www.police.hu/a-rendorsegrol/testulet/teruleti-szervek/keszenleti-rendorseg> (Letöltve: 2019. 03. 02.)

Jogszabályok

1994. évi XXXIV. törvény a rendőrségről (2019. március 02-i állapot)

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (2019. március 02-i állapot)

1998. évi XIX. törvény a büntetőeljárásról /hatályon kívül/ (2019. március 02-i állapot)

2009. évi CLV. törvény a minősített adat védelméről (2019. március 02-i állapot)

2012. évi C. törvény a büntető törvénykönyvről (2019. március 02-i állapot)

2017. évi XC. törvény a büntetőeljárásról (2019. március 02-i állapot)

295/2010. (XII. 22.) kormányrendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól (2019. március 02-i állapot)