KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT

XVII. évfolyam 1. szám 2019. március

SZAKMAI SZEMLE

ALAPÍTVA: 2003

BUDAPEST

A Katonai Nemzetbiztonsági Szolgálat
tudományos-szakmai folyóirata

Felelős kiadó

Dr. Béres János altábornagy, főigazgató

Elérhetőségeink

Postacím:	Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa 1111 Budapest, Bartók Béla u. 24-26. 1502 Budapest, Pf. 117
Telefon:	Dr. Kenedli Tamás 30/738-7925 Simon László 30/999-5205
E-mail:	szakmaiszemle.kontakt@gmail.com
Weblap:	http://www.knbsz.gov.hu/hu/publikaciok.html

HU ISSN 1785-1181

TARTALOM

Tisztelt Olvasó!
Tisztelt Szerzőink!
Tisztelt Lektoraink!

A Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle elnevezésű folyóiratának szerkesztőbizottsága 2019. évi lapszámainak tartalmával szeretne megemlékezni az idén **70 éves Észak-atlanti Szerződés Szervezetében** betöltött tagságunk időszakáról. Tudományos lapunkban igyekszünk elhelyezni a témában jártas neves szakértők írásait, konferenciákon elhangzott előadásokat, katonai vezetők külszolgálatok alkalmával szerzett tapasztalatait. Fontos számunkra, hogy megismertessük olvasóinkkal a 70 éve megalakult NATO létrejöttének történeti és politikai körülményeit, a Magyar Honvédség útját a NATO-ba, valamint ehhez kapcsolódóan a katonai hírszerzés és elhárítás szakmai kapcsolatainak, történetének alakulását és a jelenlegi helyzetét.

Az utolsó néhány évben olyan változások következtek be a kibertérrel összefüggő kérdéskörökben nemzetközi színtéren, amelyek már az EU-s és NATO követelmények síkján is nemzeti szintű reagálásokat követelnek. Amikor a nemzeti vagy ágazati szintű kommunikációs képességek biztonságos használatáról, igénybevételéről beszélünk, az információbiztonsági kérdések tanulmányozása megkerülhetetlen. Jelenleg a kibertérben tapasztalható fenyegetések, a szolgáltatásokban, termékekben feltárt sérülékenységek a korábbihoz képest nagyságrendekkel emelik a felhasználók veszélyeztetettségi szintjét. A magyar kibervédelmi keretrendszer a szabályozás és felelősségi körök tekintetében több ponton módosult. A **katonai kibertér műveleti képességek**re vonatkozó követelmények, illetve a képességfejlesztés szempontjából is nagyon fontos a nemzeti és katonai stratégiai szinten bekövetkezett változások megértése, lekövetése, az újabb beavatkozást igénylő témakörök feltárása és megfelelő ellenlépések tervezése. Mindennek érdekében nagyon sokat tehetnek a Szakmai Szemlében is publikáló, kutatói szemlélettel rendelkező, gyakorlatorientált szakemberek. Kérjük őket, hogy írásaikkal segítsék elő a szakmai ismeretterjesztést.

A jubileumi évre helyezett fókusz mellett, hagyományos rovatainkat – az MTA mértékadó folyóiratok jegyzékében szereplő besorolásunkra tekintettel – továbbra is minőségi szakmai írásokkal szeretnénk feltölteni, ezért kérjük meglévő és jövőbeli szerzőinket, hogy az alábbi rovatok témáira tekintettel tervezzék publikációs tevékenységüket.

Nemzetbiztonság elmélete
(Nemzetbiztonsági rendszerek, szervezetek feladatrendszere, működése, történelme, szervezeti változásai, hazai és külföldi titkosszolgálatok, nemzetbiztonsági együttműködések, ágazati kapcsolatok, nemzetbiztonsági kockázatok kezelése, nemzetbiztonsági információk, illetve azok kapcsolódása, védelem-igazgatás és a válságok kezelése);

Biztonság- és védelempolitika
(Állam- és jogtudomány érintkező területei, országismeret, külföldi szolgálatok, fegyveres testületek, idegen hadseregek, nemzeti és szakági stratégiák, doktrínák, direktívák, NATO szabályok és szabványok, azok hatásai, válságkezelő és nemzetközi műveletek, gyakorlatok ezen belül katonai, rendészeti, katasztrófavédelmi, pszichológiai és szociális tevékenységek nemzetbiztonsági vetületei);

Technikai rendszerek
(Nemzetközi és hazai titkosszolgálati és titkos információgyűjtő tevékenységet befolyásoló információ- és haditechnika, geoinformatika, kiberműveletek és -védelem stb.);

Alkalmazott nemzetbiztonsági-elhárító ismeretek
(A hírszerzés és az elhárítás műveleti tapasztalatai, objektum- és rendezvénybiztosítás, nemzetbiztonsági ellenőrzés, kapcsolódó humánpolitika, rendvédelem, egészségügy és katasztrófavédelem, szervezett bűnözés elleni védelem és terrorelhárítás stb.);

Fórum
(alkalmazható állam-, jog- és hadtudomány, vallástudomány stb.);

Továbbá recenziók, hírek, események, konferenciák, kapcsolódó adatok.

A beérkező publikációk szakmai ellenőrzése során jövőben is törekszünk tudományos minősítéssel rendelkező személyek bevonására, igényességgel látjuk el a szakmai cikkek lektorálását. Mindezzel hozzá kívánunk járulni az egyetemi hallgatók, doktoranduszok és doktorjelöltek szakmai felkészültségének növeléséhez, a témavezetők munkájának megkönnyítéséhez.

Ezúton is kívánunk sikeres alkotómunkát és eredményes együttműködést valamennyi partnerünk számára.

A szerkesztők:

Dr. Kenedli Tamás ezredes PhD
felelős szerkesztő
a KNBSZ Tudományos Tanácsának
titkára
☏+36-30/738-7925

Simon László alezredes
felelős szerkesztő
a KNBSZ Tudományos Tanácsának
tagja
☏+36-30/999-5205

Elérhetőség:
szakmaiszemle.kontakt@gmail.com

SZŰCS LÁSZLÓ

SZÍRIA ÉS AZ ISZLÁM ÁLLAMNAK NEVEZETT TERRORSZERVEZET EGYEDI VONÁSAI 2018-IG

Bevezetés

> *„A terrorizmus az erőszak kiszámított alkalmazása bizonyos politikai, vallási, vagy ideológiai célok elérése érdekében. A terrorizmussal együtt jár bizonyos bűncselekmények elkövetése, amely gyakran szimbolikus természetű, és a közvetlen áldozatokon túl a közönségre kíván hatást gyakorolni."*
>
> Brian Jenkins – Rand Corporation

A szunnita szélsőséges csoportoknak – amelyek a politikai rendszer megváltoztatásáért harcolnak és jogokat követelnek – az amerikai invázió Irakban és az azt követő szíriai polgárháború termékeny talajt kínált a terjeszkedésre. A 2014-ben megalakított Iszlám Állam (Iraki és Levantei Iszlám Állam vagy Iraki és Szíriai Iszlám Állam, a továbbiakban: ISIS) is egy ilyen szervezet. Az ISIS, mint terrorszervezet rendkívül sikeres: jól szervezett, jól finanszírozott, és ezidáig az egyik legveszélyesebb nemzetközi terrorszervezet.

Az ISIS – kihasználva az Irakban és Szíriában kialakult helyzetet – eredeti célja egy kalifátus létrehozása volt Szíria és Irak szunnita többségű területein, majd később egyesíteni kívánta Jordániát, Izraelt, Palesztinát, Libanont, Ciprust és Törökország déli részét.

A nemzetközi terrorizmus megjelenése

Szakértők szerint a modern terrorizmus a második világháború után jött létre, amikor az európai nagyhatalmak gyarmatain „gyarmatellenes" nacionalista csoportok jelentek meg. Ezen nacionalista csoportok felismerték, hogy terrortámadások útján befolyásolhatják a politikát.[1]

Az 1960-as és 1970-es években a szélsőbaloldali illetve a szélsőjobboldali ideológiát követő terrorszervezetek akciói révén megjelent a köztudatban a „nemzetközi terrorizmus" fogalma. 1972. szeptember 5-én – a müncheni olimpián – a „Fekete Szeptember" nevű palesztin terrorszervezet izraeli sportolókat ejtett túszul

[1] Max ROSER – Mohamed NAGDY – Hannah RITCHIE: Terrorism. 2018. https://ourworldindata.org/terrorism, p. 2. (Letöltés ideje: 2018. 03. 03.)

és végzett ki, ami felhívta a világ közvéleményének, valamint a kormányoknak a figyelmét a terrorizmus óriási veszélyére és nemzetközivé válására.[2]

Az elmúlt évtizedekben fokozódott a terrorizmus politikai célú felhasználása. A 2001. szeptember 11-ei terrortámadás-sorozat fordulópont volt a világtörténelemben, és ennek következtében a „terrorizmus elleni harc/háború" fogalma is része a mindennapoknak. A repülőgépekkel elkövetett pusztítás során – becslések szerint – 3000 embert öltek meg, ami az emberi történelem leghalálosabb terrorista támadásaként került be a történelemkönyvekbe. A szeptember 11-e után elkövetett terrortámadások – Moszkvában, Spanyolországban, Londonban, Törökországban, Franciaországban stb. – világossá tették az állami vezetők előtt, hogy a nemzetközi terrorizmus terjedése következtében szükségessé vált, hogy a nemzetközi közösség is szorosabban együttműködjön annak érdekében, hogy megfékezzék, illetve ellehetetlenítsék ezen szervezetek működését.[3]

Annak ellenére, hogy növekszik azon országok száma, amelyek aktívan és fegyveresen is fellépnek a terrorizmussal és annak bármilyen támogatásával szemben, számottevő állam még mindig támogatja azt.[4] Egyes társadalmak nem akarják nyíltan, illetve nem képesek teljes mértékben érdekeiket érvényesíteni. A terrorista szervezeteken keresztül ezen államok elérhetik akár politikai, akár gazdasági céljaikat is. Példaképpen fel tudnánk hozni a Hezbollah-t, amelyet Irán hozott létre és folyamatosan támogat. Ezen felül megemlíthetjük Pakisztánt is: a Dzsamaat ul-Ahrár terrorszervezetet támogatva Pakisztán folyamatosan bomlasztja Indiai belső összetartását, ezáltal sikeresen akadályozza Dzsammu és Kasmír állam integrálódását Indiába.[5]

1. Az ISIS

Az ISIS Irakban, alapvetően az al-Kaida terrorcsoporthoz köthető szélsőséges szervezetekből alakult ki. A 2004-es amerikai iraki megszállás után az ISIS elődszervezetének „egyszerű" dolga volt. Összefogta azokat az al-Kaida-szimpatizánsokat, akik hajlandóak voltak tovább folytatni a harcot az Egyesült Államok ellen. Eleinte sok szakértő úgy vélekedett, hogy az ISIS csak egy újabb „átlagos" terrorista szervezet, azonban idővel bebizonyosodott, hogy mindennek nevezhető, de nem átlagosnak. Ma már kijelenthető, hogy az ISIS nem más, mint az al-Kaida egy szélsőséges szakadár csoportja.

Az ISIS hivatalosan 2014-ben alakult meg, azonban előzményeinek története 1999-ig nyúlik vissza. Az ISIS megalakulása óta több nevet is felvett, aminek egyik oka a terrorszervezet éppen aktuális hovatartozásának jelzése volt:

---

2 RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban. Zrínyi Kiadó, 2013, p. 14.

3 Uo.

4 JÓZSA László: Globális terrorizmus – Válaszok a terrorizmusra. SVKH-Chartapress, Budapest 2002. p. 93.

5 RESPERGER – KISS – SOMKUTI i. m. p.87.

- Dzsamjat at-Tauhid wal-Dzsihad
- al-Kaida Iraki frakciója (al-Qaeda in Iraq/AQI)
- Iraki ISIS (The Islamic State in Iraq/ISI)
- Iraki és Szíriai ISIS (The Islamic State in Iraq and Sham/ISIS/ISIL)
- ISIS (Islamic State/IS)

Az ISIS „elődszervezete", a Dzsamjat at-Tauhid wal-Dzsihad 2003-ban Irakban harcolt a koalíciós erők ellen. 2004-ben hűséget esküdtek Osama bin Ladennek, és megváltoztatták a nevüket az al-Kaida iraki frakciójára, aminek az élén Abu Musab al-Zarkawi állt. 2006-ban Zarkawi áldozatul esett egy légitámadásnak és helyét Abu Bakr al-Bagdadi vette át. A terrorszervezet 2008-ban az Iraki ISIS, majd az Iraki és Szíriai ISIS nevet vette fel. Miután a szervezet belépett a szíriai polgárháborúba, igényét (a már elfoglalt iraki területeken kívül) kiterjesztette Szíria szunnita többségű területeire is. 2014. június 29-én megalapították a kalifátust, Abu Bakr al-Bagdadi[6] lett a kalifa és a csoport felvette az ISIS nevet.[7]

1. ábra: Az ISIS lobogója
forrás: http://worldofdrjustice.blogspot.hu/2014/09/flagge-verbot.html
(Letöltés ideje: 2018.01.09)

Nagy Imre: *„A szíriai konfliktus (2011-2017) dinamikája – A polgárháború jellegének és tartalmának átalakulása"* című tanulmányában összefoglalja azokat a tényezőket, amik lehetővé tették az ISIS felemelkedését:

- *„a szír vezetés maga manipulálta az iszlám fundamentalistákat: felhasználta őket Irakban, majd saját határain belül – gyengítve és lejáratva a mérsékeltebb ellenzéki erőket, ugyanakkor a „terrorizmus elleni harc"-al igazolva tetteit;*

---

6 Abu Bakr al-Bagdadi egy iraki származású terrorista, aki korábban az Al-Káida tagja volt. 2010 és 2014 között az ISIS „emírjeként" tartották számon, majd 2014 júniusában – a kalifátus magalakulását követően – kinevezte magát kalifának.

7 NAGY Imre: A szíriai konfliktus (2011-2017) dinamikája – A polgárháború jellegének és tartalmának átalakulása. ZKE-NPT, szakdolgozat, 2017. p. 56.

- *a szaddami elnyomással összekapcsolt kollektív bűnösség vádja a kirekesztő politikával és a síita milíciák bevonása a harcokba Irakban és Szíriában elidegenítette a szunnita lakosság jelentős részét, akik önvédelemből csatlakoztak a mesterségesen keltett síita-szunnita szembenállást pusztító belháborúvá fejlesztő legszélsőségesebb irányhoz;*
- *a meggyengült központi hatalom és a megosztott ellenzéki erők miatti vákuum kihasználásának lehetősége."*[8]

1.1. Az ISIS célja

Az ISIS a szunnita iszlám VII. századi hagyományait követi (szalafizmus), mely elvet minden más értékrendet, hagyományt és vallást.[9] Az ISIS ideológiája szerint helyre kell állítani a kalifátust, amit egy kalifa irányít a saría vallásjogi hagyományainak megfelelően, és ezt csakis a dzsihádon keresztül lehet megvalósítani.

A dzsihád az iszlám vallás szerint egy kollektív kötelezettség, a közhiedelemmel ellentétben a dzsihád nem jelent erőszakot vagy szent háborút. A terrorista szervezetek által elkövetett cselekmények ellentmondanak az iszlám vallás számos tanításának, törvényének. Az ISIS a dzsihádot az alábbiak szerint értelmezi: *a dzsihád egyéni kötelesség, minden hithű muszlim kötelessége, és felhatalmazza a hívőket, hogy az iszlám nevében a földrajzi helyzetétől függetlenül csatlakozzon a globális iszlám ellenálláshoz, amelynek a legfőbb ellensége a nyugati világ, az általa képviselt értékekkel együtt, és elpusztítása érdekében terrorcselekményeket is végrehajthatnak.*[10]

Harmat Árpád Péter *„Az ISIS legvégső célja"* című publikációjában három valószínűsíthető végső célt határozott meg az ISIS vonatkozásában: [11]

- a szunnita szalafizmus erőszakos terjesztése az egész világon;
- a nyugati típusú berendezkedés (államfelépítés, hatalomgyakorlás, demokrácia, jogrend stb.) meggyengítése és felszámolása;
- profitszerzés.

Több tanulmány is foglalkozik az ISIS törekvéseivel, amelyek alapján a fentiekben felsorolt célokkal kapcsolatban a szakértők között egyetértés mutatkozik. Így kijelenthetjük, hogy az ISIS legvégső célja a *„civilizációrombolás, mely egyeduralkodóvá teszi a Földön a szunnita vallás legszélsőségesebb irányzatát, miközben meggazdagítja az Iszlám Állam vezetőit és befektetőit."*[12]

---

8 Uo. p. 56

9 HARMAT Árpád Péter: Az ISIS legvégső célja. 2016. 08. 09., Pervenimus.blog.hu/2016/08/09/az_isis.legvegso_célja (Letöltés ideje: 2018. 04. 01.)

10 Migrációkutató Intézet elemzése: Az önkéntes vakság ára – gyorselemzés a párizsi terrortámadást követően. 2015. november 16. https://www.migraciokutato.hu/hu/2015/11/16/az-onkentes-vaksag-ara-gyorselemzes-a-parizsi-terrortamadast-kovetoen/ (Letöltés ideje: 2018. 02. 16.)

11 HARMAT i. m.

12 Uo.

1.2. Az ISIS felépítése és vezetése

Abu Bakr al-Bagdadi (a kalifa) az ISIS önjelölt vezetője, akit egyben Mohamed próféta utódaként tartottak számon.[13] Az ISIS, ami korábban egy militáns terrorszervezet volt, egy kvázi „önkormányzati" szervezetté fejlődött, amely a lakosság részére általános szolgáltatásokat is nyújtott. Az ISIS elég nagy területet (közel 83.000 négyzetkilométer) vont a fennhatósága alá, és emiatt nehéz egy személynek központilag irányítania. Al-Bagdadi az ISIS irányítását csakis decentralizálással tudta megoldani. Abdulrahman Musztafa al-Kaduli a szervezet szíriai helytartója, míg Abu Muszlim al-Turkmani pedig az iraki kormányzója, egyben al-Bagdadi helyettesei voltak. A végrehajtó hatalmat al-Bagdadi és kabinetének tanácsadói, valamint két helyettese, al-Kaduli és al-Turkmani alkották.[14]

Al-Bagdadi katonai tapasztalatokkal rendelkező személyeket alkalmazott a vezetésben: két helyettese, al-Anbari és al-Turkmani – akik egyben az ISIS Biztonsági Tanácsának két vezetője voltak – korábban az iraki hadseregben szolgáltak.[15]

Az ISIS legfelső tanácskozó testülete a Shura Tanács volt. Az ISIS operatív irányítását egy három főből álló kormány és háborús kabinet végezte, ezen felül létrehozták a pénzügyi, politikai, jogi, katonai, külföldi harcosok ügyei, biztonsági, hírszerzési, médiaügyek szakigazgatási tanácsát. A biztonsági tanácson belül működött a független katonai, a civil és a vallási igazgatás, amely egyben magába foglalta a saría-intézményeket és vallási rendőrséget is.[16] A decentralizálás érdekében az ISIS vezetése 13 tartományt, azon belül körzeteket is létrehozott. Ezen tartományok és körzetek élére kijelölt személyek elszámolási kötelezettséggel tartoztak az ISIS központi vezetés felé, egyben a források újraelosztásáért is feleltek.[17]

---

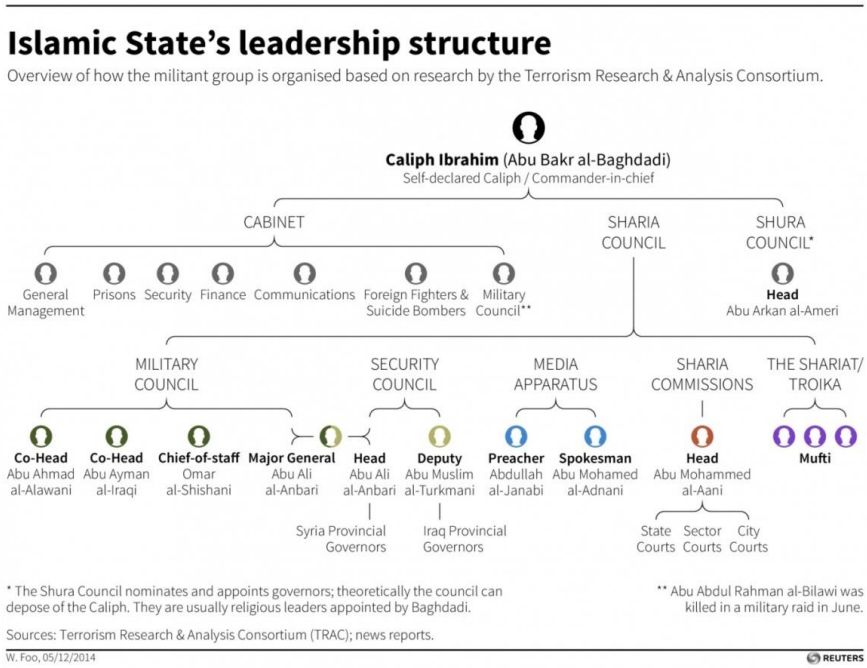
[13] A koalíciós erők 2017 júliusában csapást mértek al-Bagdadi konvojára, és eleinte a sajtó ki is jelentette, hogy az ISIS vezetője meghalt. Ezt azonban sem az USA, sem más nemzet nem erősítette meg. A Reuters információ szerint a terrorszervezet számos vezetője meghalt a légicsapás során, azonban al-Bagdadi nem volt köztük. 2017 szeptemberében napvilágra került egy hangfelvétel is, melyben al-Bagdadi nyilatkozott.

[14] TOPOLÁNSZKY Ádám: Az ISIS terrorszervezet anatómiája. MNO, 2014. október 1. http://mno.hu/nezopontok/az-iszlam-allam-terrorszervezet-anatomiaja-1250721 (Letöltés ideje: 2018. 02. 06.)

[15] Uo.

[16] NAGY i. m. p. 59.

[17] NAGY i. m. p. 60.



2. ábra: Az ISIS vezetési struktúrája lobogója
forrás: http://www.ibtimes.co.uk/isis-leadership-whos-who-fluid-islamic-state-structure-power-1509014 (Letöltés ideje: 2017. 12. 12.)

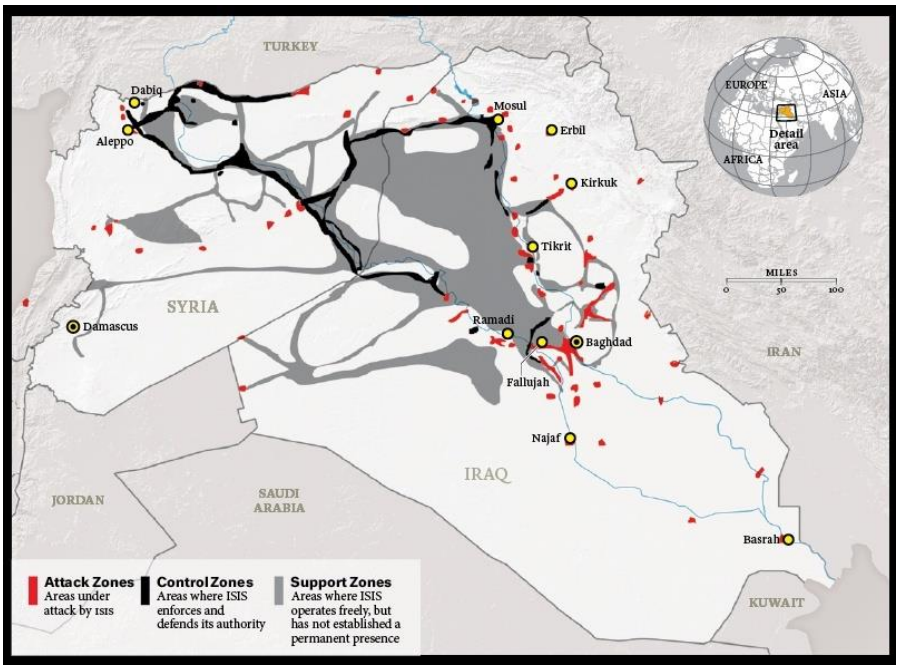
Al-Bagdadi két helyettese irányította a tizenhárom szíriai és iraki tartományt a kormányzókon keresztül, akik az utasításokat a helyi tanácsoknak továbbították. Az ISIS kabinetje – ami a szervezet napi ügyeit irányította – hét miniszterből állt. A Shura Tanács – amely egyenesen a végrehajtó hatalomnak tartozott beszámolási kötelezettséggel – a kalifátus vallási ellenőrző szerve is volt egyben. Elsőszámú feladata volt, hogy a helyi tanácsok és kormányzók az ISIS akaratának megfelelően hajtsák végre az iszlám törvénykezést. A Shura Tanács az ISIS vezetőségét is felülbírálhatta, amennyiben valamelyik döntésük nem felelt volna meg a saría törvénykezés követelményeinek.[18]

Az ISIS kiemelt figyelmet fordított a jogszolgáltatás ellenőrzésére. Három különböző területet különböztethetünk meg[19]:

- *Díwán al-Hisbah tanács, amely a vallási rendőrség által felterjesztett ügyekben jár el;*
- *Iszlám Bíróságok, amelyek az ISIS által alkotott törvények megszegői ellen hajtanak végre intézkedéseket;*
- *Sérelmek Bírósága, ahol szükség esetén az ISIS harcosai és parancsnokai ellen foganatosítanak intézkedéseket.*

[18] TOPOLÁNSZKY i. m.
[19] BESENYŐ János – PRANTNER Zoltán – SPEIDL Bianka – VOGEL Dávid: Az ISIS terrorizmus 2.0. Kossuth Kiadó, 2016., p. 58.

Az ISIS jól összehangolt szervezettségére utal az a tény, hogy az elfoglalt területek közigazgatási irányítását pontosan megtervezte, majd sikeresen kivitelezte. Az ISIS az elfoglalt területeken élő lakosokat a kalifátus állampolgárainak tekintette, akikért felelősséggel tartoztak.[20] A szervezet nagy hangsúlyt fektetett az elektromosság és a folyóvíz ellátásának biztosítására, továbbá intézkedéseket tettek a kommunális hulladék elszállítására is, így az elemi szolgáltatások is biztosításra kerültek. Számos kórházat létesítettek, utakat építtettek, és megnyitottak – csak fiúknak – iskolákat.[21]



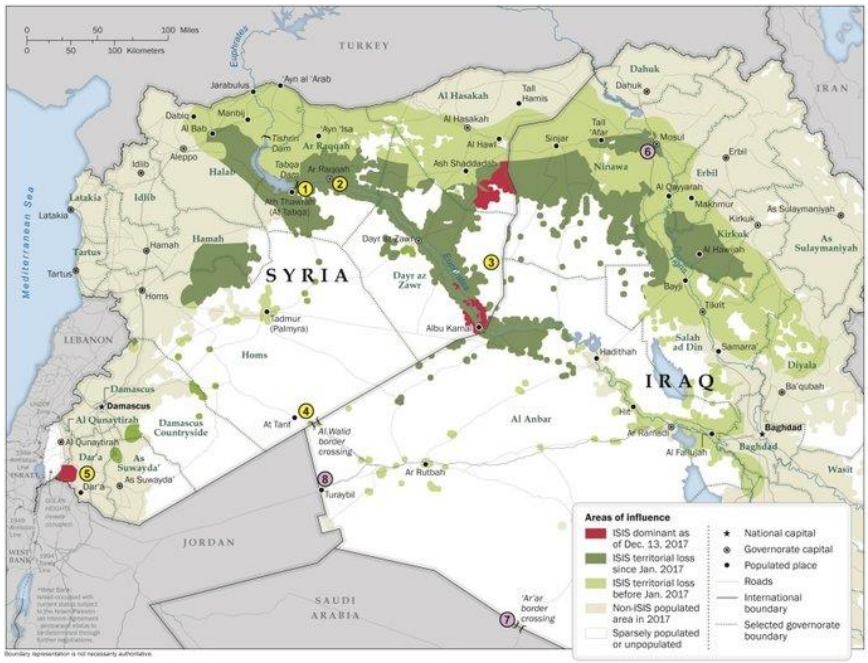
3. ábra: Az ISIS által kontrolált területek Szíria és Irak területén 2015-ben
forrás: Graeme Wood: What ISIS Really Wants. The Atlantic,
http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/
(Letöltés ideje: 2018. 04. 02.)

A térkép az ISIS által 2015-ben Irakban és Szíriában elfoglalt és kontrollált területeket mutatja be. Az általuk felügyelt területeken található kórházakat, iskolákat, üzemeket, olajkutakat és a telekommunikációs infrastruktúrákat is sikerült fennhatóságuk alá vonni, továbbá az ISIS saját adókat vettet ki az ott élő lakosokra. Ez azonban 2017-ben radikálisan megváltozott. A nemzetközi fellépésnek köszönhetően 2017-re az ISIS elvesztette a korábban megszerzett területei felett az irányítást.

Az Egyesült Államok külügyminisztériuma által 2017-ben nyilvánosságra hozott térkép szerint az ISIS meghatározó szerepet játszott három szíriai területen: Szíria délnyugati részén, közel az izraeli határhoz; Szíria keleti részén, közel a

[20] TOPOLÁNSZKY i. m.
[21] HAHNER Péter: Az Iszlám Állam. Rubicon Kiadó, 2016, p. 24.

szíriai és iraki határhoz; valamint Szíria észak-nyugati részén, a kurdok által ellenőrzött területek közelében.



4. ábra: Az ISIS által kontrolált területek Szíria és Irak területén 2017-ben
forrás: http://www.businessinsider.com/map-of-isis-territory-2017-12
(Letöltés ideje: 2018. 04. 02.)

Látható, hogy 2015 és 2017 között az ISIS elvesztette iraki és szíriai területeinek több mint 90%-át. Az amerikai külügyminisztérium elemzése szerint az ISIS harcosainak nagy része ebben az időszakban Törökországban lelt menedékre.

1.3. Az ISIS forrásai

A kalifátus működése érdekében az ISIS vezetése 2015-re közel kétmilliárd dolláros költségvetést fogadott el. Ezt a költségvetést az elfoglalt területeken élőkre kivetett adókból, valamint külföldi támogatásokból biztosította a szervezet. Az ISIS továbbá saját bankokat hozott létre, valamint fizetőeszközként arany-, ezüst- és rézpénzt használtak. Az ISIS által létrehozott bankok hitel-szolgáltatásokat is kínáltak, ami hosszú távú pénzbevételi forrást jelentett a szervezet számára. Azonban a költségvetésük jelentősebb részét a kőolaj feketepiaci értékesítéséből fedezték. [22]

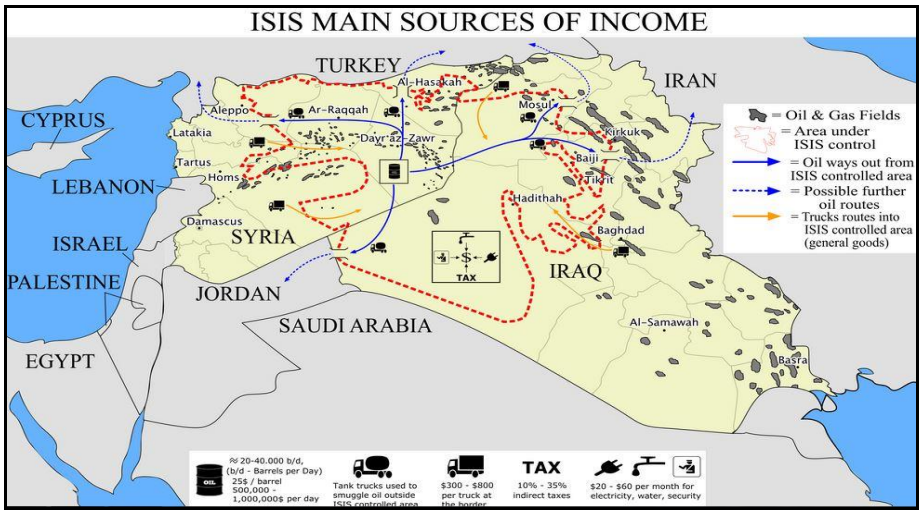
[22] SIMON Péter – SZALONTAI Gábor: A „Természetes Megoldás" Fedőnevű Nemzetközi Művelet Első Évének Értékelése. Felderítő Szemle, XIV. évfolyam 3. szám, 2015, pp. 74-75.

Az ISIS bevételének többsége az energia termeléséből és értékesítéséből származott. Az ISIS közel 350 olajkutat működtetett Irakban és Szíriában: Szíria olajkitermelésének közel 60%-a az ISIS kezében volt. Az ISIS által elfoglalt olajmezőkből kitermelt és illegálisan eladott olaj több tízmillió dollárt hozott a szervezetnek az utóbbi években: becslések szerint 2013-ban közel napi 1 millió dollár, 2014-ben már napi 3 millió dollár folyt be az ISIS-hez olajeladásokból. Az olaj nagy részét illegálisan Törökországban értékesítették.

2015 közepére az ISIS elvesztette az irányítást a három legnagyobb olajmező felett. Annak ellenére, hogy az Egyesült Államok által végrehajtott légicsapások elsődleges célpontjai az ISIS műveleti központjai, kiképzőtáborai, fegyverzeti és haditechnikai raktárai, valamint ellenőrzőpontjai voltak, a légicsapások során célba vették – pénzügyi forrásainak elapasztása érdekében – az ISIS által ellenőrzött kőolajmezőket és üzemanyag-szállító gépjárműveit is.[23] Ez jelentősen csökkentette az ISIS olajértékesítéséből származó bevételét. Azonban fontos megjegyezni, hogy az olajeladáson kívül az ISIS a Szíriában elfoglalt erőművekből származó villamos energiát is értékesítette.[24]

Az olajkitermelésen kívül az ISIS egyik legnagyobb pénzbevételi forrása az illegális drogkereskedelemből származik. Egyes szakértők szerint a terrorszervezet a drogexport révén évi szinten közel 1 milliárd dollár bevételhez jutott.

A fentiek alapján megállapítható, hogy a történelem során az ISIS az egyik leggazdagabb és legjobban finanszírozott terrorszervezet volt.



5. ábra: Az ISIS pénzügyi forrásai
forrás: https://moneyjihad.files.wordpress.com/2015/03/isis-income-map.jpg
(Letöltés ideje: 2017. 12. 20.)

---

[23] SZALONTAI Gábor: A szíriai polgárháború okozta regionális menekültváltság és hatása az európai migrációs helyzetre. Felderítő Szemle, XIV. évfolyam 3. szám, 2015, p. 82.

[24] Max FISHER: How ISIS is exploiting the economics of Syria's civil war; 2014. 06. 14.; https://www.vox.com/2014/6/12/5802824/how-isis-is-exploiting-the-economics-of-syrias-civil-war (Letöltés ideje: 2018. 01. 18.)

1.4. Az ISIS sikerének okai a térségben

Számos tényező járult hozzá az ISIS térnyeréséhez és terjedéséhez 2018-ig. Az iraki és szíriai válság helytelen kezelése, valamint a radikális politikai iszlám és a növekvő dzsihádizmus mind növelhették eredményességüket.

Az egyik legjelentősebb tényező az volt, hogy az ISIS az iraki konfliktus és a szíriai polgárháború okozta politikai űrt sikeresen kihasználta, így 2014-ben Szíria és Irak jelentős területeit nagyon rövid idő alatt el tudta foglalni. A szervezeti fegyelem és az elfoglalt területeken az állami szolgáltatások azonnali megszervezése és folytatása is hozzájárult ahhoz, hogy 2014. június 29-én kikiáltásra került a kalifátus, a csoport pedig felvette az ISIS nevet.[25]

Robert A. Pape szerint az ISIS rendkívüli gyors sikere négy fő tényező párhuzamos bekövetkezésének eredménye volt:
Az ISIS megnyerte az iraki szunnita lakosság támogatását, ami elősegítette az ISIS gyors terjedését, főleg Irak szunnita területein. Az ISIS gyors terjedését a 2010-es iraki parlamenti választások is segítették: az Iraqiyya szunnita koalíció nyerte meg az elektorális választásokat, de az Egyesült Államok közbenjárásával a síita koalíció nyerte meg a választásokat.[26] Az ezt követő politikai leszámolások és letartóztatások, ami felháborodást keltett az iraki szunnita lakosság körében, és így ismét rengetegen álltak az ISIS mellé.

Továbbá az ISIS harcosai motiválatlan és legyengült iraki hadsereg ellen harcoltak, így sikerült stratégiailag fontos helyszíneket és objektumokat elfoglalnia.[27]

Kiemelendő, hogy az ISIS képes volt kulcsfontosságú természeti erőforrásokat elfoglalni Szíria és Irak területén. Ezen erőforrások révén teljes mértékben képes volt finanszírozni saját működését. Ezen felül a terrorszervezet az elfoglalt területeken saját Központi Bankot hozott létre, valamint saját arany-, ezüst- és rézpénz kiadását kezdeményezték.[28]

Az ISIS gyors térnyerésének, sikerének negyedik oka az eredményes közösségi médiában folytatott tudatos program volt. Ennek a kampánynak a legfőbb célja a toborzás, valamint az adományok és az anyagi segélyek megszerzése és begyűjtése volt.[29]

---

[25] TRENCSÉNI Dávid: Honnan jött az ISIS; 2016. szeptember 10. http://vs.hu/kozelet/osszes/honnan-jott-az-iszlam-allam-0910#!s0 (Letöltés ideje: 2018. 03. 01.)

[26] Robert A. PAPE – Sarah MORELL: Four reasons for ISIS's success. http://blog.oup.com/2015/01/reasons-isis-islamic-state-success (Letöltés ideje: 2017. 12. 30.)

[27] Uo.

[28] Uo.

[29] Uo.

1.5. Az ISIS harcosai

Az ISIS fegyveresei nagyobb részt az adott országban élőkből, valamint számos külföldi önkéntesből álltak. 2018-ig több közel-keleti, nyugat-európai és amerikai muzulmán csatlakozott hozzájuk. A szíriai területeken kívül számos – a Közel-Keleten, Közép-Ázsiában és Észak-Afrikában működő muszlim dzsihádista csoport csatlakozott, illetve biztosíotta támogatásáról az ISIS-t. [30]

Különböző nemzetközi szervezetek becslései szerint az ISIS a rendkívül jól szervezett toborzó tevékenységének köszönhetően kb. 200.000 harcossal rendelkezett. Az ISIS tagjai között számos 20-30 év közötti fiatal található, akik többsége nem rendelkezett felsőfokú végzettséggel.[31] Többségük főleg iraki és szíriai származású férfi volt, akik korábban már együttműködött és/vagy tagja volt az al-Kaida terrorszervezetnek. Sokukat az ISIS fenyegetés vagy erőszak útján kényszerített arra, hogy harcoljon az oldalukon. Ezen felül az ISIS az elfoglalt területeken számtalan toborzóirodát is működtetett. A jelentkezést követően az illető vallási és katonai felkészítésen vett részt, és csak ezek után küldték harcba.[32]

Az ISIS az interneten, és azon belül a különböző közösségi média portálokon is folytatott toborzótevékenységet, és ennek eredményeként folyamatos volt a külföldi harcosok érkezése. Nemzetközi szervezetek becslése szerint az ISIS-hez több mint 30.000 külföldről érkezett személy csatlakozott, melyek közül egyes becslések szerint 5000-6000 főre tehető azoknak a száma, akik valamelyik NATO-tagállamból és/vagy nyugati országokból érkeztek a Közel-Keletre.[33]

1.6 Külföldi harcosok

Az ISIS-hez számos országból érkeztek külföldi harcosok, akik elsősorban politikai vagy ideológiai okok miatt csatlakoztak a terrorszervezethez. Ez nem új jelenség: egyes szakértők szerint 1980 és 2010 között vélhetően 10.000-30.000 ilyen egyén csatlakozott a muszlim országokban zajló különféle fegyveres konfliktusokhoz.[34]

Az Egyesült Államok hírszerző szolgálataitól származó adatok szerint 2015-ben több mint 100 országból közel 30.000 külföldi harcos érkezett Szíriába és Irakba, többségük muzulmán országokból.[35] Csak Európából több mint 6000 főre tették számukat: többségük Nagy-Britanniából, Franciaországból, Belgiumból, Törökországból és az Egyesült Államokból érkeztek. Továbbá egyes becslések szerint közel 5000 főre tehető azok száma, akik a szovjet utódállamokból (a Kaukázus és Közép-Ázsia régió országaiból) érkeztek a szervezethez. Az ISIS-hez

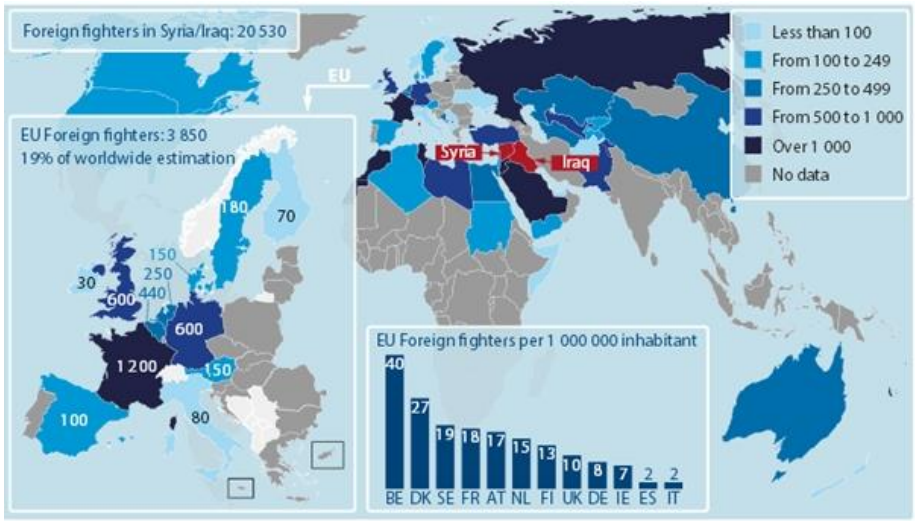
---

30 BESENYŐ– PRANTNER– SPEIDL– VOGEL i. m. p. 21.
31 Uo. p. 16.
32 Uo. p. 17.
33 Uo.
34 Migrációkutató Intézet elemzése: Az önkéntes vakság ára – gyorselemzés a párizsi terrortámadást követően. 2015. november 16. https://www.migraciokutato.hu/hu/2015/11/16/az-onkentes-vaksag-ara-gyorselemzes-a-parizsi-terrortamadast-kovetoen/ (Letöltés ideje: 2018. 02. 16.)
35 KIS-BENEDEK József (2017): Dzsihadista fészkek, mint a terrorizmus lehetséges kiindulópontjai. http://mhtt.eu/hadtudomany/2017/2017_1-2/HT_2017_96-113.pdf

csatlakozó külföldi harcosok száma folyamatosan változott. Statisztikai adatok szerint 2014-ben 81 országból 12 ezer külföldi harcos állt az ISIS mellé, 2015 decemberére már 27-31 ezer közötti külföldi harcos 84 országból került ki.[36]

Azonban az egyes hírügynökségek által készített statisztikák nem beszélnek arról, hogy hány külföldi harcos tervezte a kiutazást, továbbá hányan lehettek, lehetnek azok, akik a saját országukban működtek együtt, illetve támogatják jelenleg is az ISIS-t. Példaként megemlíthetjük Afganisztánt, Algériát, Szenegált, Jement, Ománt vagy Pakisztánt, ahol szinte képtelenség akár megbecsülni is ezen fegyveresek számát.[37]

A külföldi harcosok motivációját tekintve két csoportot azonosíthattunk. Az egyik csoportba azok tartoztak, akik hisznek az ISIS céljaiban és részesei akarnak lenni az új kalifátus kialakításának. A másik csoportját azok a személyek képezték, akik kizárólag kalandvágyból csatlakoztak a szervezethez.



6. ábra: Az Európából származó külföldi harcosok
Forrás: https://www.migraciokutato.hu/hu/2015/11/16/az-onkentes-vaksag-ara-gyorselemzes-a-parizsi-terrortamadast-kovetoen/ (Letöltés ideje: 2018. 02. 16.)

Az ISIS-hez csatlakozott külföldi harcosokat azonnal bevonták a harccselekményekbe. Az iszlám kiképzők a „nyugati harcosokat" kezdetben öngyilkos merényletekre használták, mivel jóval kevesebb megbecsülést kaptak az arab származású és arabul beszélő társaikkal szemben. Később az ISIS vezetősége azonban rájött, hogy hatékonyabb a külföldről érkező harcosokat kiképezni, majd visszaküldeni az anyaországukba. Ennek egyik célja valószínűsíthetően az volt, hogy a nyugati országokban alvó-sejteket hozzanak létre, akik az utasítást követően készen állnak különböző terrorcselekményeket végrehajtani.[38]

---

36 Uo.
37 ZSEBE Zsolt: Külföldi harcosok az Iszlám Állam mellett, Nemzet és Biztonság 2015/1. szám, p. 24.
38 NAGY i. m. p. 61.

A külföldi országokból csatlakozó harcosok rendkívül motiváltak voltak és rövid felkészítést/képzést követően azonnal bevethetőkké váltak. Amennyiben az egyéni fegyveres harcra nem voltak alkalmasak, úgy felhasználhatták más feladatokra is, mint például üzenetetek küldésére, illetve a propaganda terjesztésére.[39]

Ezeknek a külföldi harcosoknak a radikalizálása nem egyik napról a másikra történt. A radikalizálódásnak négy fázisát különböztetjük meg: az első fázis az elő-radikalizáció, amely során az egyén hajlandóságot mutat az iszlám szélsőségesek iránt. Ezt követi az önazonosulás időszaka, majd az oktatás fázisa. Az utolsó fázis a dzsihadistává válás időszaka, amely során elkezdődik a merénylet tervezése és a feladatra történő felkészülés.[40]

2013 és 2015 között az ISIS internetes propagandahálózatának és toborzókampányának köszönhetően nagymértékben megnőtt a hozzájuk csatlakozó külföldi harcosok száma. Az ISIS a propagandatevékenységének nagy részét az interneten, és ezen belül a különböző közösségi oldalakon végezte, amelynek legfőbb célcsoportja a nyugati országokban élő muszlimok voltak. Természetesen az ISIS „klasszikus" toborzása – amely során vallási közösségekben, mecsetekben, valamint börtönökben toboroztak fiatal muzulmánokat – szintén folyamatos volt.

1.7. Az ISIS propagandagépezete

„Négy fő célt különböztetünk meg a terroristák médiahasználatában: az első a propagandájuk közzététele és a félelemkeltés megvalósítása, a második a nagyobb (általában anyagi) támogatás megmozgatása a szervezetük számára, a harmadik lejáratni a kormányokat és mindazokat a szervezeteket, akiknek kötelességük lett volna megvédeni az állampolgárokat, a negyedik pedig további támadásokat inspirálni, akár más szervezetek részéről, akár a saját szervezetükbe való toborzással."[41]

Az utóbbi évtizedben rendkívüli fejlődést tapasztalhattunk az informatika és a kommunikációs hálózatok terén, ezáltal már nem csak a fejlett országokban, de már a világ harmadik országaiban is elérhető a szélessávú internet az „okos" infokommunikációs eszközökön keresztül.[42]

Az internet adta lehetőségek az ISIS egyik legfontosabb eszközévé vált, segítségével szabadon, ellenőrzés nélkül kommunikálták propagandájukat. Az ISIS volt az első olyan terrorszervezet, mely hatékonyan, teljes mértékben kihasználta az internet és a közösségi média adta lehetőségeket.[43] Az interneten folytatott

---

[39] KIS-BENEDEK József (2016): Dzsihadizmus, Radikalizmus, Terrorizmus; Zrínyi Kiadó, 2016. p. 90.

[40] Uo. p. 84.

[41] ISTVÁNFFY András: A terrorizmus, mint rituális kommunikáció; http://beszelo.c3.hu/cikkek/a-terrorizmus-mint-ritualis-kommunikacio (Letöltés ideje: 2018. 03. 16.)

[42] SZABÓ András: Az Aszimmetrikus hadviselés nemzetbiztonsági kihívásai; NKE KNT, 2016. p. 30.

[43] ROSER –NAGDY –RITCHIE i. m. p. 2.

propagandatevékenységet nyugaton tanult szakemberek vezették, amely a kiadványok, honlapok, videók minőségén is jól látható.[44]

Az internet segítségével az ISIS a fiatal szimpatizánsok százezreit szólította meg. Az ISIS a közösségi médián keresztül érte el a legtöbb személyt. A Facebook, Twitter és hasonló közösségi oldalakon keresztül az ISIS-nek lehetősége volt arra, hogy felvegye az érdeklődőkkel és a potenciális csatlakozókkal a kapcsolatot.[45] Az ISIS online-toborzás céljából létrehozta a „*Dabiq"* című online magazinját is. Az Interneten gyakorlatilag szabadon, ellenőrzés nélkül terjednek még ma is a szélsőséges megnyilvánulások és propagandák. Ezek rendkívül veszélyes fegyvernek minősíthetők az iszlamisták kezében.[46]

Következtetések

Az ISIS fegyveresei 2017-ben és 2018-ban már súlyos vereségeket szenvedtek el Irakban és Szíriában. Az Oroszországi Föderáció és az Egyesült Államok által vezetett koalíció egyidejűleg végrehajtott támadásai teljes mértékben legyengítették a terrorszervezetet. Szíriában és Irakban az ISIS által kontrollált földrajzi területek, a bevételeik, valamint harcosainak száma is folyamatosan csökkent. Az Egyesült Államok vezetése 2018 decemberében hivatalosan is bejelentette, hogy kivonulnak Szíriából, annak ellenére, hogy nem sikerült teljes mértékben felszámolni a terrorszervezetet. A biztonságpolitikai szakértők szerint az ISIS propaganda- és médiaapparátusa azután is működőképesen fennmarad, hogy az ISIS katonai erejének „teljes felszámolása" bekövetkezne. Az ISIS megmaradt tagjai és szimpatizánsai más területeken (akár földrajzi, fizikai vagy információs környezetben) is folytatják magányos és csoportos harcukat.

Mi jelenthet akkor megoldást? A történelem korábbi jelentős terrorszervezeteit sem sikerült teljesen legyőzni. A szervezet fegyveres küzdelmének, működésének ellehetetlenítése nem számolja fel az ideológiai, valamint politikai konfliktusokat. A harcosok más terrorszervezethez csatlakozhatnak, esetleg sajátot hozhatnak létre. A hagyományosnak tekinthető társadalmi, politikai, katonai, környezeti és technikai szegmensekben az – ISIS esetében eddig kiemelten tapasztalt – információs aktivitás új fegyverek és módszerek alkalmazását vetítik előre a terrorizmus elleni küzdelemben. Ezen egyedi vonások azonosítása egyértelműen határozzák meg a további gyakorlati megoldások és tudományos kutatások fókuszát.

---

[44] Loretta NAPOLEONI: Az iszlamista főnix – Az ISIS születése és Közel-Kelet újrafelosztása; HVG Kiadó Budapest, 2015. p. 105.

[45] Masi ALESSANDRIA: ISIS Recruiting Westerners: How The 'Islamic State' Goes After Non-Muslims And Recent ConvertsIn The West; http://www.ibtimes.com/isis-recruiting-westerners-how-islamic-state-goes-after-non-muslims-recent-converts-west-1680076, (Letöltés ideje: 2018. 02. 04.)

[46] Migrációkutató Intézet elemzése: Az önkéntes vakság ára – gyorselemzés a párizsi terrortámadást követően; 2015. november 16. https://www.migraciokutato.hu/hu/2015/11/16/az-onkentes-vaksag-ara-gyorselemzes-a-parizsi-terrortamadast-kovetoen/ (Letöltés ideje: 2018. 02. 16.)

Felhasznált irodalom:

- ALESSANDRIA, Masi: ISIS Recruiting Westerners: How The 'Islamic State' Goes After Non-Muslims And Recent ConvertsIn The West; http://www.ibtimes.com/isis-recruiting-westerners-how-islamic-state-goes-after-non-muslims-recent-converts-west-1680076, (Letöltés ideje: 2018. 02. 04.)
- BENKE József: Az arabok története; Kossuth Könyvkiadó, Budapest, 1987.
- BESENYŐ János, PRATNER Zoltán, SPEIDL Bianka, VOGEL Dávid: Az ISIS terrorizmus 2.0; Kossuth Kiadó, 2016.
- BHAT Abdul Manan: Hafez al-Assad, Controlling Syria from the Grave; World News, 2016.06.11. https://intpolicydigest.org/2016/06/11/hafez-al-assad-controlling-syria-from-the-grave/ (Letöltés ideje: 2018. 02. 01.)
- BORBÉLY Tamás – BORBÉLY Attila: Az EUfóriától az EUtanáziáig? Migránsok, emigránsok, menekültek; Polgári Szemle, 2015. december 4-6. szám
- CONWAY Medaline: Timeline: U:S: approach to the Syrian civil war. Politico; 2017. 07. 04. https://www.politico.com/story/2017/04/timeline-united-states-response-syria-civil-war-237011 (Letöltés ideje: 2018. 03. 11.)
- CSICSMANN László: Iszlám és demokrácia a Közel-Keleten és Észak-Afrikában; Dialóg Campus Kiadó, Budapest, 2008.
- CSONKA Anna: Milyen volt az élet Szíriában a háború előtt? 2015. 10. 13.; Index, https://index.hu/nagykep/2015/10/13/sziria_a_haboru_elott/ (Letöltés ideje: 2018. 02. 17.)
- DR. BÉRES János: Muszlim Radikalizmus Nyugat-Európában; Felderítő Szemle, XV. évfolyam 4. szám, 2016. pp. 5-31.
- FERWAGNER Péter Ákos – KOMÁR Krisztián – SZÉLINGER Balázs: Terrorista szervezetek lexikona; Maxim Könyvkiadó, Szeged, 2003.
- FISHER, Max: How ISIS is exploiting the economics of Syria's civil war. Vox; 2014. 06. 14.; https://www.vox.com/2014/6/12/5802824/how-isis-is-exploiting-the-economics-of-syrias-civil-war (Letöltés ideje: 2018. 01.18.)
- GYIMESI Roland: Az arab tavasz geopolitikai háttere; ELTE Természettudományi Kar, Szakdolgozat, 2014.
- HANKISS Ágnes: A „magányos farkas" legendája – Terrorista hálózatok. Arc és Álarc; I. évfolyam 2–3. szám, Hamvas Intézet, 2017, p. 206.
- HARMAT Árpád Péter: Az ISIS legvégső célja; 2016. 08. 09., Pervenimus.blog.hu/2016/08/09/az_isis.legvegso_célja (Letöltés ideje: 2018. 04. 01.)
- HERMANN, Rainer: Az ISIS – A világi állam kudarca az arab világban; Akadémia Kiadó, Budapest, 2015.

- HJELMGAARD, Kim: Syrian conflict explained: How did we end up here?, USA Today, 2018. 04. 09. https://www.usatoday.com/story/news/world/2018/04/09/syria-conflict-explained-bashar-assad/498756002/ (Letöltés ideje: 2018. 04. 15.)
- ISTVÁNFFY András: A terrorizmus, mint rituális kommunikáció; http://beszelo.c3.hu/cikkek/a-terrorizmus-mint-ritualis-kommunikacio (Letöltés ideje: 2015. 07. 14.)
- J. NAGY László: Az arab országok története a XIX-XX. században; Eötvös József Könyvkiadó, Budapest, 1997.
- JAKUS János: A terrorizmus elleni küzdelem általános megítélése; KBH Szakmai Szemle, 2003/I. szám. pp. 21-41.
- JÓZSA László: Globális terrorizmus: fogalmi keretek – Válaszok a terrorizmusra; SVKH-Chartapress, Budapest 2002.
- KIS-BENEDEK József: A terrorizmus ellen folytatott hírszerzés; http://www.zmne.hu/dokisk/hadtud/hirszerzes.pdf (Letöltés ideje: 2015. 12. 13.)
- KIS-BENEDEK József: Az Iszlám Kalifátus és a globális dzsihád új tendenciái; Hadtudomány, Budapest 2014/3-4. szám pp. 22-33.
- KIS-BENEDEK József: Dzsihadista fészkek, mint a terrorizmus lehetséges kiindulópontjai; http://mhtt.eu/hadtudomany/2017/2017_1-2/HT_2017_96-113.pdf
- KIS-BENEDEK József: Dzsihadizmus, Radikalizmus, Terrorizmus; Zrínyi Kiadó, 2016.
- KOROM Mária: Az iszlám radikalizmus térnyerése a nyugat-balkánon; Migrációkutató Intézet, 2016. https://www.migraciokutato.hu/hu/2016/05/17az-iszlam-radikalizmus-ternyerese-nyugat-balkanon/ (Letöltés ideje: 2018. 03. 01.)
- Migrációkutató Intézet elemzése: Az önkéntes vakság ára – gyorselemzés a párizsi terrortámadást követően. 2015. november 16. https://www.migraciokutato.hu/hu/2015/11/16/az-onkentes-vaksag-ara-gyorselemzes-a-parizsi-terrortamadast-kovetoen/ (Letöltés ideje: 2018. 02. 16.)
- NAGY Imre: A szíriai konfliktus (2011-2017) dinamikája – A polgárháború jellegének és tartalmának átalakulása; ZKE-NPT, 2017.
- NAPOLEONI , Loretta: Az iszlamista főnix – Az ISIS születése és Közel-Kelet újrafelosztása; HVG Kiadó Budapest, 2015.
- NÓGRÁDI György: Nemzetvédelem Szögesdróttal – A migrációs vállság és magyar vonatkozásai; KNBSZ Felderítő Szemle, XV.évfolyam 1. szám
- PAPE Robert A. – MORELL Sarah: Four reasons for ISIS's success; http://blog.oup.com/2015/01/reasons-isis-islamic-state-success (Letöltés ideje: 2017. 12. 30.)
- PERROW, Charles: Szervezetszociológia; Osiris Kiadó, Budapest, 1997.

- RESPERGER István Az erőszak helye szerepe az Iszlám Állam terrorszervezet tevékenységében; Hadtudományi szemle, 2015. VIII. 4. szám
- RESPERGER István, Kiss Álmos Péter, Somkuti Bálint: Aszimmetrikus hadviselés a modern korban; Zrínyi Kiadó, 2013.
- REUTER, Christoph: Az ISIS: a fekete hatalom és a terror stratégiái; Művelt Nép Kiadó, Budapest, 2016.
- ROSER, Max – NAGDY, Mohamed – RITCHI, Hannah E.: Terrorism; 2018. https://ourworldindata.org/terrorism; p. 2. (Letöltés ideje: 2018. 03. 03.)
- ROSTOVÁNYI Zsolt: Az iszlám a 21. század küszöbén; Aula Kiadó, Budapest, 1998.
- ROSTOVÁNYI Zsolt: Az iszlám világ és a Nyugat; Corvina Kiadó, Budapest, 2004.
- SEIB, Philip – JANBEK, Dana M.:, Global Terrorism and New Media, The post-Al Qaeda generation; New York, Routledge.
- SELOOM, Muhanad: az ISIS és az európai menekültválság; Migrációkutató Intézet, 2015. november 21.; https://www.migraciokutato.hu/hu/2015/11/21/az-isis-es-az-europai-menekultvalsag/ (Letöltés ideje: 2018. 01. 06.)
- SIMON Péter – SZALONTAI Gábor: A „Természetes Megoldás" Fedőnevű Nemzetközi Művelet Első Évének Értékelése; Felderítő Szemle, XIV. évfolyam 3. szám, 2015.
- SÓGOR Dániel: Országismertető – Szíria; Zrínyi Kiadó, 2013.
- SÓTÉR László: Szíria jelentősége az Amerikai Egyesült Államok és Oroszország szemszögéből; ZKF-NPT, szakdolgozat.
- SZABÓ András: Az Aszimmetrikus hadviselés nemzetbiztonsági kihívásai. NKE-KNT, diplomamunka, 2016.
- SZALONTAI Gábor: A szíriai polgárháború okozta regionális menekültváltság és hatása az európai migrációs helyzetre. Felderítő Szemle, XIV. évfolyam 3. szám, 2015
- TÁLAS Péter – VARGA Gergely: Stratégiai törekvések a szíriai válság kapcsán II. Nemzet és Biztonság, 2013/1-2. szám. pp. 66-86.
- TARJÁN G. Gábor: A terrorizmus történelmi dimenziói. Belügyi Szemle, BM Kiadó, 2002 pp. 6-7.
- TOPOLÁNSZKY Ádám: Az ISIS terrorszervezet anatómiája. MNO, 2014. október 1. http://mno.hu/nezopontok/az-iszlam-allam-terrorszervezet-anatomiaja-1250721 (Letöltés ideje: 2018. 02. 06.)
- TRENCSÉNI Dávid: Honnan jött az ISIS. Vs.hu, 2016. szeptember 10. http://vs.hu/kozelet/osszes/honnan-jott-az-iszlam-allam-0910#!s0 (Letöltés ideje: 2018. 03. 01.)
- WEISS, Michael – HASSAN, Hassan: Az ISIS- A terror hadserege belülről. HVG Kiadó, Budapest, 2015.

- WOOD, Graeme: What ISIS Really Wants. The Atlantic, Március 2015.
- ZSEBE Zsolt: Külföldi harcosok az Iszlám Állam mellett, Nemzet és Biztonság 2015/1. szám.
- Graeme Wood: What ISIS Really Wants. The Atlantic, http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/ (Letöltés ideje: 2018. 04. 02.)
- http://web.colby.edu/contemporary-issues/as-about-us/ (Letöltés ideje: 2018. 01. 11.)
- http://worldofdrjustice.blogspot.hu/2014/09/flagge-verbot.html (Letöltés ideje: 2018.01.09)
- http://www.bbc.com/news/world-middle-east-27838034 (Letöltés ideje: 2017. 12. 11.)
- http://www.bbc.com/news/world-middle-east-27838034 (Letöltés ideje: 2017. 12. 11.)
- http://www.bbc.com/news/world-middle-east-27838034 (Letöltés ideje: 2017. 12. 11.)
- http://www.businessinsider.com/map-of-isis-territory-2017-12 (Letöltés ideje: 2018. 04. 02.)
- http://www.ibtimes.co.uk/isis-leadership-whos-who-fluid-islamic-state-structure-power-1509014 (Letöltés ideje: 2017. 12. 12.)
- http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/ (Letöltés ideje: 2017. 12. 12.)
- https://moneyjihad.files.wordpress.com/2015/03/isis-income-map.jpg (Letöltés ideje: 2017.12.20.)
- https://www.migraciokutato.hu/hu/2015/11/16/az-onkentes-vaksag-ara-gyorselemzes-a-parizsi-terrortamadast-kovetoen/ (Letöltés ideje: 2018.02.16.)
- https://www.migraciokutato.hu/hu/2015/11/16/az-onkentes-vaksag-ara-gyorselemzes-a-parizsi-terrortamadast-kovetoen/ (Letöltés ideje: 2018.02.16.)
- Syria crisis: where key countries stand, http://www.bbc.com/news/world-middle-east-23849587, 2015. 10. 30. (Letöltés ideje: 2018.01.03.)
- https://www.thoughtco.com/definition-of-the-arab-spring-2353029 (Letöltés ideje: 2018. 01. 03.)
- Syria's civil war explained from the beginning https://www.aljazeera.com/news/2016/05/syria-civil-war-explained-160505084119966.html (letöltés: 2018.01.16.)

DR. BODA MIHÁLY

A CIA HIDEGHÁBORÚS TEVÉKENYSÉGÉNEK ÚJRAÉRTÉKELÉSE – 1. RÉSZ
A TPAJAX-MŰVELET ELSŐ MEGKÖZELÍTÉSBEN ÉS AZ OLAJÉRDEKEKRE TÁMASZKODÓ MAGYARÁZAT[1]

I. Bevezetés

A titkosszolgálatok és a hírszerző szolgálatok hidegháborús fedett akcióinak, különösen a TPAJAX-nak a vizsgálata manapság időszerű és fontos feladat. Egy ilyen vizsgálatnak legalább kétféle jelentősége lehet. Fontos lehet abban a szűk értelemben, hogy a vizsgálat által többet tudunk meg a vizsgált fedett akcióról vagy az azt végrehajtó titkosszolgálat vagy hírszerző szolgálat tevékenységének jellemzőiről. Fontos lehet azonban egy olyan általánosabb nézőpontból is, amelyben a vizsgált fedett akció nem csupán történelmi relevanciával rendelkezik, hanem olyan általános relevanciával is, amely alapján a vizsgálatból messzebb ható, akár a mára is kiterjedő következtetéseket lehet levonni.

A TPAJAX-művelet a CIA által 1953 augusztusában az iráni miniszterelnök, Mohammed Moszadek[2] ellenében végrehajtott puccs. A TPAJAX mai vizsgálatának az kölcsönöz különleges, ám szűkebb jelentőséget, hogy 2017-ben az amerikai kormány nyilvánossá tette azoknak a dokumentumoknak a nagy részét, amelyek a puccs előzményeként, a puccs alatt és a puccs utóéleteként keletkeztek. Ezeknek a forrásoknak a feldolgozása alapjaiban hozzájárulhat a TPAJAX céljának, mibenlétének és módszereinek a megértéséhez.

A TPAJAX vizsgálata azonban fontos egy általánosabb nézőpontból is. Jelenkorunk az újra felélénkülő hidegháborús (vagy ahogy manapság nevezik: hibrid háborús) tevékenységek korszaka, amelyben különleges szerep jut a nemzetbiztonsági szolgálatoknak. Talán a felélénkülő hidegháborús tevékenység részeként kell felfogni a migrációs krízist Németországban kihasználó orosz nemzetbiztonsági tevékenységet, az amerikai, francia és talán egyéb parlamenti és elnökválasztást manipuláló tevékenységet, illetve a 2016 őszén Montenegróban politikai puccs végrehajtására irányuló tevékenységet. Azért csak „talán”, mert ezeknek az akciónak a lezajlásáról és hátteréről, lévén titkos akciók, nem sokat tudunk. A hagyományos hidegháborús fedett akciók vizsgálata azonban hozzásegíthet bennünket ahhoz, hogy olyan célokat és módszereket ismerjünk meg, amelyek nem csupán a hagyományos hidegháborúban voltak érvényesek, hanem más történelmi időszakokban is érvénnyel rendelkeznek, így a hidegháborús fedett akciók jellemzése mellett felhasználhatjuk a kortárs fedett akciók jellemzésére is.

Tanulmányom elsősorban a szűkebb célt igyekszik megvalósítani, azaz nem törekszem a fedett akciók céljainak vagy módszereinek általában vett felderítésére,

[1] A tanulmány elkészítésében nyújtott segítségért köszönettel tartozom Pál Istvánnak.

[2] A perzsa nevek átírásában felhasználtam: LIGETI Lajos (szerk.): Keleti nevek magyar helyesírása; Budapest, Akadémiai Kiadó, 1981.

ugyanakkor írásomat annak a szem előtt tartásával készítettem el, hogy az továbbfejleszthető legyen az általánosabb cél irányába.

A tanulmány három részből áll, ebben az első részben először bemutatom a „TPAJAX" akroníma jelentésének lehetséges feloldásait, majd röviden az 1953. augusztusi iráni puccs eseményeit, majd felállítom a CIA fedett műveletei számára egy többkomponensű osztályozási rendszert, végül megfogalmazom a tanulmány további részének azt a keretállítását, hogy az 1953. augusztusi iráni puccs kapcsán érdemes kizárólag az Egyesült Államok érintettségét vizsgálni, ezen belül is azt, hogy az USA központi hírszerző szolgálata, a CIA miért vagy milyen indokkal vállalt oroszlánrészt puccsban. Ezeket követően, még mindig az első részben, bemutatom a puccsnak a szakirodalomban található egyik, a tanulmány szempontjából lényeges, ám hagyományosnak tekinthető magyarázatát. Ez a hagyományos magyarázat arra épít, hogy az USA-nak (és rajta keresztül Nagy-Britanniának) az iráni olajforrások megszerzésére/megtartására voltak komoly törekvései. A tanulmány második és harmadik része az iráni puccs további magyarázataival foglalkozik.

II. TPAJAX: az első pillantás

1. Az elnevezés: „TPAJAX"

A puccs elnevezésével abban a formában is lehet találkozni, hogy AJAX, ám a CIA-művelet elnevezésének teljes formája a CIA dokumentumaiban „TPAJAX". A „TPAJAX" elnevezés két részre bontható, a „TP"-re és az „AJAX"-ra. A „TP" egy prefixum, amelyet háromféleképpen is szokás értelmezni a szakirodalomban. Az első értelmezés szerint a „TP" a CIA Iránra vonatkozó kódja, aminek értelmében egyetlen Iránban zajló CIA-akció elnevezése sem nélkülözheti a „TP" prefixumot. Így a TPAJAX-ot megelőző CIA-akció, a TPBEDAMN nevében is szerepel. Más országokban zajló akciók értelemszerűen más kódot kaptak.[3] Egy másik, bár az elsővel összeegyeztethető megközelítés szerint a „TP" azért utal Iránra, és azért szerepel a „TPBEDAMN" és a „TPAJAX" kódokban, mert ezek az akciók valamilyen formában az iráni kommunista párt, a Tudeh párt (angolul Tudeh Party) ellen irányultak, amely párt nevének rövidítése szerepel a CIA-akciók kódjában is.[4] Végül a harmadik értelmezés szerint, a „TP" a „Target Practice" rövidítése, amivel a rövidítés arra utal, hogy a kiválasztott célpontot meg kell semmisíteni (az „AJAX" megfelelő értelmezésének megfelelően).[5]

A „TPAJAX" név második része az „AJAX" eredete sem sokkal világosabb, mint az első részé. A prefixum után álló elnevezéseket illetően a brit hírszerzési szervezet, az SIS, kutatója, Philip Davies szerint a hírszerzési akciók fedőneveit az 50-es években az ügynökök már nem a saját fantáziájuk szerint választották, hanem

---

[3] WILFORD, Hugh: America's Great Game – The CIA's Secret Arabists and the Shaping of the Modern Middle East; New York, Basic Books, 2013., p. 166.

[4] GASIOROWSKI, Mark J.: The CIA's TPBEDAMN Operation and the 1953 Coup in Iran; In Journal of Cold War Studies (15), 2013., p. 10. 11. lábjegyzet

[5] RAHNEMA, Ali: Behind the 1953 Coup in Iran; Cambridge, CUP, 2015., p. 61.

azokat egy előre adott véletlenszerű listából rendelték a műveletekhez.[6] Amennyiben ez így is volt a brit gyakorlatban, az amerikai eljárás valószínűleg más volt. A TPAJAX elnevezés eredetéről illetően ugyanis legalább két elképzelés is létezik.

Az AJAX-művelet a nevét – Tim Weiner szerint – a Trójánál küzdő görög hősről kapta, akinek a magyar neve Aiasz. Mivel Aiaszból a homéroszi eposzban kettő is volt, nagy Aiasz (Telamon fia) és kis Aiasz (Oileusz fia), ezért amennyiben a művelet neve tényleg a görög hős nevéből származik, akkor nem világos, hogy melyik Aiaszról is van szó. Az elnevezéssel kapcsolatban Weiner megjegyezte, hogy az *„eléggé furcsa választás volt, mivel a legenda szerint Aiász elborult elmével lemészárolt egy birkanyájat abban a hitben, hogy ellenséges harcosok, majd miután észhez tért, szégyenében öngyilkos lett”*.[7] Weiner így nagy Aiaszként értelmezte AJAX-ot, és Roosevelt elnöknek tulajdonította a névadást.[8] Ha kis Aiaszként gondolunk a művelet névadójára, akkor csak egy kicsivel szerencsésebb a művelet helyzete, mivel kis Aiasz a híres-hírhedt trójai falóban ülő különítmény tagjaként elhurcolta Kasszandrát Pallasz Athéné templomából és megerőszakolta, amiért isteni bosszúként hajótörésben halt meg.

A másik elképzelés az „AJAX” név választására a homéroszi eredethez képest igencsak prózai. Hugh Wilford szerint ugyanis a CIA-akció egyszerűen a háztartási tisztítószertől kölcsönözte a nevét, amivel a névadók arra kívántak utalni, hogy az akcióval megtisztítják Iránt a kommunistáktól.[9]

2. Az események: felmerülés, jóváhagyás, tervezés, lezajlás – az első pillantás

A TPAJAX-művelet először 1952 őszén merült fel a CIA berkein belül, ekkor még név nélkül, csak mint fedett („speciális politikai”) akció.[10] Az akció a következő év tavaszán konkretizálódott több lépésben: először a CIA igazgatója bocsátott a teheráni CIA-kirendeltség rendelkezésére 1 millió $-t arra az esetre, ha bele kellene avatkoznia az iráni belpolitikába, majd május közepén a CIA és a brit hírszerzési szolgálat (SIS) képviselői Cipruson (Nicosiában) fektetették le a most már TPAJAX-nak nevezett akció alapjait, amit júniusban Bejrútban, majd London konkretizáltak. A CIA, az SIS és az USA külpolitikai vezetése június végén hagyta jóvá a tervet, az USA és Nagy-Britannia elnöke pedig július elején.

A művelet végrehajtásában komoly szerepe volt az iráni uralkodónak, Mohammed Reza Pahlavi sahnak és a sahhoz hű katonai vezetőknek. A sah többszöri megkeresés után is csak akkor volt hajlandó komolyan részt vállalni az eseményekben, ha világosan látja, hogy Eisenhower és Churchill elnökök is támogatják azt. A művelet kezdetét ezért olyan rádióbeszédek előzték meg az amerikai és a brit elnök részéről, amelyeknek egyes részletei jelezték a sah számára

---

6 DAVIES, Philip: MI6 and the Machinery of Syping; London and Portland (OR), Frank Cass, 2004., p. 226.

7 WEINER, Tim: A CIA története 104. o., Budapest, GABO, 2009.

8 Uo.

9 WILFORD i. m. p. 166.

10 NSC 136/1 4.g. In FRUS 1952-1954, Iran, 1951-1954, United States Government Publishing Office Washington, 2017.

a támogatást.[11] A sah támogatása mellett az olyan iráni katonai vezetők hűsége is kiemelkedően fontos volt, mint Záhedi tábornok, a császári testőrség, illetve a teheráni katonai ezredek tisztjei.

A művelet lényegi része azzal kezdődött, hogy a sah aláírt két királyi határozatot („firman”-t), amelyekkel egyrészt menesztette Mohammed Moszadeket a miniszterelnöki pozícióból, másrészt kinevezte Záhedi tábornokot ugyanebbe a pozícióba. A „firman”-okat augusztus 15-én késő este akarták kézbesíteni az érintetteknek a császári testőrség segítségével. Moszadek azonban a császári testőrségben lévő besúgói révén értesült az akcióról, így nem ő vette át a neki szóló „firman”-t, hanem egy beosztottja, és letartóztattatta az azt kézbesítő tisztet, Naszeri ezredest. Naszeri letartóztatását számos, a sahhoz hű katonai vezető letartóztatása is követte, Záhedi tábornokot azonban elrejtette a CIA, a sah pedig, aki egyébként is a Kaszpi-tengeri királyi üdülőben tartózkodott, Bagdadon keresztül Rómába menekült. Másnap reggel Moszadek a rádióban bejelentette, hogy puccsot kíséreltek meg ellene, a puccs azonban megbukott.

A CIA teheráni kirendeltségének vezetője, Kermit Roosevelt ekkor úgy döntött, hogy más úton érik el a kitűzött célt, Moszadek hatalmon kívül helyezését. Roosevelt először megköröztette a nyugati, majd azon keresztül az iráni sajtóban a sah által aláírt „firman”-okat, és eljutatta azokat a vidéki katonai táborokba, illetve a fizetett helyi ügynökök segítségével Moszadek-ellenes hangulatot igyekezett kelteni az utcán. Ennek keretében provokátorokat is felhasználva kommunista tüntetést szervezett, amelyhez nemsokára nagyszámban csatlakoztak a Tudeh párt szimpatizánsai. A tüntetés olyan mértékeket öltött, hogy a tüntetők már a Pahlavi család szobrait rombolták, és kiáltványban álltak ki a népköztársaság mellett. Ekkor, augusztus 18-án, az teheráni amerikai nagykövet, Loy Henderson felkereste Moszadeket, hogy tájékozódjon a kialakult helyzetről, illetve, hogy figyelmeztesse az iráni miniszterelnököt, a Tudeh párt tüntetői USA-ellenes hangulatot keltenek, amelyben a teheráni amerikaiak nincsenek biztonságban. Henderson arra kérte Moszadeket, hogy tegyen valamit a helyzet normalizálásáért, mert ellenkező esetben az USA kénytelen lesz evakuálni állampolgárait, és leállítani az Iránnak nyújtott segélyt. Moszadek erre a baloldali tüntetők ellen kivezényelte – a hagyományosan a sahhoz hű – rendőröket és katonákat, és feloszlatta a tüntetést. A következő napon a CIA fizetett ügynökei és provokátorai segítségével sah-párti tüntetést szervezett, amelyhez a megismert „firman”-ok hatására csatlakoztak a vidéki katonai táborok egységei, és a helyei rendőrség és katonaság nagy része is. A tüntetés során aztán a Záhedihez hű katonaság augusztus 19-én délutánra fegyveres harcban elfoglalta Moszadek házát, és elfogta magát Moszadeket is. Délután Záhedi tábornok bejelentette, hogy a sah által kinevezett legitim miniszterelnökként átvette a hatalmat Teheránban és Iránban. A harcok összesen körülbelül 300 halálos áldozattal jártak.

[11] ROOSEVELT, Kim: Coutercoup; New York, McGraw-Hill Book Company, 1979., pp. 156-157.

3. A TPAJAX a CIA műveletein belül

a. A CIA születése

Az Egyesült Államoknak háborús időkben az 1770-es évek közepétől mindig is volt katonai hírszerzési szervezetei, sok esetben nem is egy, hanem a minisztériumoknak vagy a fegyvernemeknek megfelelően több, azonban ezek a szervezetek sem voltak képesek megakadályozni vagy előre jelezni a Pearl Harbor-i katasztrófát. A második világháború után ezért az az elképzelés alakult ki, hogy szükség van egy olyan civil hírszerzési szervezetre, amelynek az egyik feladata a meglévő hírszerzési szolgálatok munkájának koordinációja és összesítése. A második világháborút követően az USA-ban a centralizációval képzelték el a Pearl Harborhoz hasonló meglepetésszerű támadások kiküszöbölését.

A CIA közvetett elődszervezete a második világháború alatt világszerte kiterjedten működő katonai hírszerző szervezet, a Stratégiai Szolgálatok Irodája (Office of Strategic Service, OSS) volt. Az OSS a háború alatt többek között kínai és vietnámi ellenállókat képzett ki a Távol-Keleten Japánnal szemben, illetve osztrák és német ellenállókat Európában, de szerepük volt a „lend-lease program" elindításában is.

Truman elnök 1945-ben megszüntette az OSS-t, 1946 legelején pedig létrehozta a Központi Hírszerzési Csoportot *(*Central Intelligence Group, CIG). A CIG egy rövid, és a többi hírszerzési szervezetnek való kiszolgáltatottságban töltött idő után (koordinálnia kellett volna, de nem kapott információkat) teljes önállóságra tett szert mind humán, mind anyagi forrásokban, és még az OSS-nek a világszerte kiterjedt titkos hírszerzési részlegét is hozzácsatolták (ezt akkoriban azzal a szlogennel jellemezték, hogy „egy egér megeszik egy elefántot").

1947 nyarán a nemzeti biztonságról hozott törvény (*The National Security Act of 1947*[12]) megváltoztatta a CIG nevét Központi Hírszerzési Hivatalra (*Central Intelligence Agency*, CIA), létrehozta azt a fórumot – Nemzetbiztonsági Tanács (*National Security Council,* NSC) –, amely a CIA-t az elnökkel összekötötte, és meghatározta a CIA általános célját és konkrét feladatait[13]. A CIA általános célja „a különböző kormányzati osztályok és ügynökségek hírszerzési tevékenységének koordinációja a nemzetbiztonság érdekében"; a CIA konkrét feladatai pedig a következők:

(1) tanácsot ad hírszerzési tevékenységet illetően az NSC-nek;
(2) ajánlást tesz a többi hírszerzési szervezet koordinálását illetően az NSC-nek;
(3) elemzi és értékeli a nemzetbiztonsághoz kapcsolódó hírszerzési adatokat, és gondoskodik az adatokat eljutatásáról a kormányzathoz;
(4) ha a nemzetbiztonság megköveteli, akkor maga hajt végre centralizált hírszerzési akciót;
(5) megfelel továbbá a nemzetbiztonságot érintő hírszerzéshez kapcsolódó további szerepeknek és kötelességeknek is.

---

[12] Public Law 253, The National Security Act (1947).
[13] Public Law 253, The National Security Act (1947) Sec. 102 (d) (1)-(5).

A „nemzetbiztonságot érintő hírszerzéshez kapcsolódó további szerepeknek és kötelességeknek való megfelelés" pont tette lehetővé a gyakorlatban a CIA számára a fedett akciók, vagy más néven a csendes opciók (quiet options) végrehajtását. A csendes opciók félúton helyezkedtek el a katonai (hangos opciók) és a diplomáciai (nem-opciók) tevékenység között. Az NSC először 1947 decemberében adott felhatalmazást (NSC/4, 4-A) a CIA-nak fedett akció végrehajtásához (a CIG azonban ennek előtte is folytatott hasonló akciókat).

b. Korai és késői fedett akciók

A CIA működésének korszakai megkülönböztethetők az alapján, hogy az akciók jogi szempontból milyen felhatalmazást igényeltek.

A korai időszakban a felhatalmazás az 1947-es törvény alapján az NSC kezében volt, amely az elnök tanácsadó szervezete volt, és amelynek a tagjai az elnök mellett az alelnök, a védelemi miniszter és a külügyminiszter volt. Az NSC létrehozott további albizottságokat (mint az Office of Policy Planning, az 5412 Committee, a Special Group, a 303 Committee, a 40 Committee, vagy az Operation Advisory Group), amelyek azonban vagy csak tanácsadói szereppel rendelkeztek, vagy ritkán üléseztek, vagy a költségvetés alapján hoztak döntést. Ezek a bizottságok a legtöbb esetben az NSC-tagok megbízottjait foglalták magukban, máskor azonban (mint a Kennedy Special Group-ja) kibővített formában működtek, és az üléseikre hivatalos volt még többek között a CIA igazgatója, a Vezérkari Főnökök Tanácsának (Joint Chiefs of Staff) elnöke és az elnök nemzetbiztonsági tanácsadója is.[14] Ez azt is jelentette, hogy az amerikai Kongresszus ebben az időszakban nem kapott szerepet a fedett akciók felhatalmazásában, hanem csak az elnök, ám ő is csak elvileg. A CIA működésének korai korszakát ugyanis a „plauzibilis tagadás" (plausible denial) doktrínája hatotta át, ami szerint az elnök és más magas rangú állami vezetők felelőssége akkor védhető leginkább a CIA által végrehajtott fedett akciók tekintetében, ha nem is tudnak azokról, akkor ugyanis úgy tudják letagadni azokat, hogy nem lehet őket hazugságon kapni. A korai időszakban így a CIA működéséről a gyakorlatban sok esetben sem a Kongresszusnak, sem az elnöknek nem volt tudomása.

1974 decemberében azonban a Kongresszus, kiindulva a sikertelen chilei akcióból és a belföldön folytatott hírszerzési akciókból (Watergate-botrány) elfogadta a „Hughes-Ryan" törvényt, amelynek értelmében az elnöknek írásban jóvá kell hagynia a CIA minden fedett akcióját, és arról időben (a törvényszöveg szerint „in timely fashion") informálnia kell a Képviselőház és a Szenátus erre a célra felállított bizottságait. Amennyiben az elnök jóváhagyja az akciót, akkor „finding"-ot kell kiadnia a jóváhagyásról („…*the President finds that each such operation is important to the national security of the United States*…").[15]

A törvény elfogadását követően a Szenátus 1975-ban létrehozta a Church-bizottságot a hírszerzőszolgálatok, köztük a CIA által elkövetett visszaélések kivizsgálására. A bizottság 1975 és 1976 során számos publikációban tárta fel a hírszerző szolgálatok által a második világháborút követően elkövetett olyan

[14] JOHNSON, Loch K.: America's Secret Power; Oxford, OUP, 1989. pp. 105-107.
[15] Public Law 93 559-Dec. 30. 1974, 22 USC 2422.

cselekményeket, mint a politikai gyilkosságok vagy az amerikai állampolgárok belföldi lehallgatása.[16]

1980-ban aztán olyan további módosításra is sor került, amelynek értelmében az elnöknek nem csupán „in timely fashion" kell a bizottságokat informálnia, hanem még az akció lezajlása előtt (azzal a kitétellel, hogy szükséghelyzetben elegendő a Kongresszus nyolc vezetőjét informálni).[17]

Összességében az mondható, hogy a 70-es évek közepétől a CIA-műveletek tervezésének és végrehajtásának a szabályozása jelentősen megváltozott és jelentősen szigorodott, ami alapján a 70-es évek közepén húzható egy demarkációs vonal a korai és a késői CIA-műveletek között. Az 1953-ban végrehajtott TPAJAX a korai műveletek közé tartozik.

c. Preventív, defenzív és offenzív célok

A korai CIA-műveletek tovább osztályozhatók aszerint, hogy milyen részcél elérésével kívánják védeni az USA államérdekét. Az akciók egy része preventívnek minősíthető, amennyiben elsősorban arra törekszik, hogy megakadályozza az USA-tól és a Szovjetuniótól különböző harmadik államban az amerikai érdekveszteséget (tipikusan a kommunista térnyerést); defenzívnek, amennyiben arra törekszik, hogy az USA közvetlen szomszédságában megakadályozza az amerikai érdekveszteséget; végül offenzívnak, amennyiben arra törekszik, hogy maga idézzen elő olyan változást, amely amerikai érdekek térnyerésével jár együtt.[18]

A preventív CIA-akciók paradigmapéldája a CIA 1948-as olaszországi akciója. Az akció az NSC 4/A. számú felhatalmazásával kezdődött, amely lehetőséget teremtett a CIA számára, hogy békeidőben is folytasson fedett akciókat a hasonló jellegű szovjet hadviselés ellenében.[19] Az akció keretében a CIA hatékonyan segítette az éppen hatalmon lévő olasz kereszténydemokrata pártot a hatalma megőrzéséért folytatott választási kampányban az olasz kommunista párttal, és az azt támogató Szovjetunióval szemben.[20] A segítség többek között, kezdetben (1947 őszétől), az USA gazdasági támogatásában, katonai jelenlétében és a nem-kommunista pártok választási integrációjának szorgalmazásában és szervezésében öltött testet, majd később (1948 márciusától) Trieszt visszaadásában Olaszországnak, Olaszország ENSZ-tagságának bejelentésében, illetve olyan propaganda- és pszichológiai akciókban, mint brosúrák terjesztésében és az olasz-amerikai állampolgárok propagandisztikus levélírásra való ösztönzésében, és a levelek közvetítésében az olaszországi családtagoknak. Végeredményben a kereszténydemokraták abszolút többséggel megnyerték a választást.[21]

---

16 Final Report of the Select Commettee to Study Governmental Operations with Respect to Intelligence Activities, Washington, U.S. Government Printing Office, 1976.

17 JOHNSON i. m. pp. 107-109.

18 CALLAHAN, James: Covert Action in the Cold War; 32 skk., 70 skk., London-New York, I.B. Tauris, 2010.

19 NSC/4-A (Memorandum From the Executive Secretary (Souers) to the Members of the National Security Council), https://fas.org/irp/offdocs/nsc-hst/nsc-4.htm (Letöltés ideje: 2019. 02. 08).

20 CALLANAN i. m. pp. 41-43.

21 Uo. pp. 28-32.

Az offenzív akciók egyik első példája a CIA és a brit SIS közös akciója volt Albániában 1949 és 1954 között. A BGFIEND névre keresztelt akció célja az volt, hogy egy már halatomra került és a Szovjetunió által támogatott kommunista vezetőt, Enver Hoxha-t, megfosszon a hatalmától. Albániát a partizánok szabadították fel a német megszállás alól 1944 őszén, akik a háború végén kommunista kormányt alakítottak. A CIA/SIS-művelet 1949 őszén indult, amelynek a közvetett célja az elűzött albán király, I. Zogu hatalmának a visszaállítása volt. Ennek érdekében a CIA/SIS menekült, illetve olaszországi albánokat képzett ki Máltán, majd Németországban Heidelberg mellett, és juttatott vissza a tengeren és levegőben Albánia területére, hogy ott propagandával és tevőlegesen, paramilitáris egységként is kezdeményezzenek felkelést a kommunista kormány ellen. Az akció végül a helyi körülmények, a kommunista ellenállás és a CIA/SIS-ba beépült szovjet ügynöknek köszönhetően nem járt sikerrel.[22]

Végül, a defenzív jellegű akciók közül kiemelhető a CIA 1954-es guatemalai akciója, amely az amerikai nyugati érdekszféra egy részét volt hivatva megvédeni a kommunista befolyás erősödésétől. Az akcióban a CIA az érdekszféra védelmét azzal kívánta elérni, hogy közvetve eltávolítja a hatalomból az 1950-ben megválasztott, és a feltételezések szerint kommunista eszméket valló, illetve a Szovjetunióval kapcsolatot kereső guatemalai miniszterelnököt, Jacobo Arbenz Guzmánt. A CIA két egymást követő akciót is indított Arbenz ellen, a PBFORTUNE-t és a PBSUCCESS-t. A PBFORTUNE 1952 őszén kezdődött volna, de nem valósult meg, a PBSUCCESS pedig 1954 nyarán zajlott le, illetve pszichológiai hadviselésből, valamint az amerikai légierő által támogatott és a CIA által felszerelt és kiképzett paramilitáris csoportok bevetéséből állt. Az akció kulcsa az volt, hogy már a paramilitáris támadás kezdetekor úgy állították be a hírekben a helyzetet, mintha Arbenz elvesztette volna a hatalmát, aminek következtében Arbenz lemondott.[23]

Ebben a felosztásban már távolról sem annyira egyszerű elhelyezni az iráni TPAJAX-műveletet a korai CIA-akciók között, mert amint az látható lesz alább, annak függvényében, hogy miként magyarázzuk az akciót, a TPAJAX besorolható mindhárom kategóriába.

d. Fedett akciók típusai: propaganda-, politikai, gazdasági és paramilitáris akciók

Végezetül, a korai CIA-akcióknak lehetséges még egy további osztályozása annak a fényében, hogy milyen módszerek és eszközök segítségével igyekeztek megvalósítani az USA államérdekét. Ez alapján megkülönböztethetünk propaganda- (vagy pszichológiai) akciót, politikai akciót, gazdasági akciót és paramilitáris akciót, amelyek közül a leggyakoribbak a propagandaakciók voltak (a CIA összes akciójának kb. 40%-a), majd népszerűségen ezeket követik a politikai akciók (30%), a paramilitáris akciók (20%), és végül a gazdasági akciók (10%).[24]

---

[22] Uo.: pp. 70-81.
[23] WEINER i. m. pp. 114-126.
[24] JOHNSON i. m. p. 21.

A fedett propagandaakciók az amerikai kormány hivatalos propagandáját egészítették ki, amely utóbbiért az Egyesült Államok Információs Ügynöksége (United States Information Agency) volt a felelős. A fedett propagandaakciók során a CIA helyi irodájának a vezetője a helyi médiában rejlő lehetőségeket használta ki. A helyi médiaszakemberek (pl. riporterek, rendezők, szerkesztők, producerek, operatőrök stb.) továbbították a helyi CIA irodától megkapott híreket, cserébe pedig valamilyen formában juttatást kaptak a CIA-tól. Végeredményben a helyi állampolgárok ugyanazzal a hírrel nem csupán a hivatalos amerikai forrásokból szembesültek, hanem a hozzájuk közelebb álló, és megbízhatóbbnak ítélt helyi médiából is. Az USA érdekeit közvetlenül támogató propaganda egy másik formája a nyugati kulturális anyagok – könyvek (disszidensek és nyugati szerzők könyvei), magazinok (pl. Readers Digest), újságok, vagy hangzó anyagok (pl. Szabad Európa Rádió) – terjesztése volt a CIA fizetési listáján lévő helyi állampolgárokon keresztül.

A propagandaakciók legalább háromféleképpen támogathatták az USA érdekeit. A „fehér" propaganda az USA által nyíltan elismert reklámozása volt egy, az USA számára fontos ügynek. A „fekete" propaganda olyan anyagok terjesztéséből állt, amelyek a tartalmuk vagy egyéb jellegzetességük alapján az ellenség (pl. a Szovjetunió) egy belső, és kiszivárgott anyagának tűntek. Végül, a „szürke" propaganda anyagai vagy senkinek sem, vagy egy harmadik csoportnak tulajdonított anyagokat tartalmaztak. Mindegyik esetben lehetséges volt a propaganda tartalmát igaz, hamis, vagy részben igaz/túlzó anyaggal megtölteni.[25]

A politikai fedett akciók külföldi, baráti politikusok és bürokraták pénzbeli támogatását (lefizetését, megvesztegetését) foglalta magában, akiken keresztül a CIA és az Egyesült Államok képes volt befolyást gyakorolni az adott állam politikájára, például segítve az adott politikus érvényesülését. A korábban említett 1948-as olaszországi CIA-akció a politikai akciók egyik paradigma-példája.

A paramilitáris akciók, a második legfontosabb akciók a fedett akciók típusai közül, amely „háborúszerű" akciókban vagy alacsony intenzitású háborúkban való részvételt jelentett. A részvételnek sok formája fordult elő, kezdve a gerillacsapatok pénzbeli támogatásán, a csaptok kiképzésén, fegyverrel és hadianyaggal való ellátásán át egészen a katonai tanácsadók küldéséig vagy politikai gyilkosság megrendeléséig, megszervezéséig vagy végrehajtásáig. Az első paramilitáris CIA-akció a korábban említett albániai beavatkozás volt, de a leginkább elhíresültek vélhetően a CIA-hez köthető politikai gyilkossági kísérletek voltak Arbenz guatemalai, Castro kubai, Lumumba kongói, Trujillo dominikai és Diem dél-vietnámi elnök, illetve Schneider chilei tábornok ellen.[26]

Végezetül, a gazdasági akciók alkotják arányaiban a legkisebb hányadot a CIA akcióiban, amelyeknek a célja a célállam gazdasági működésének befolyásolása, rombolása vagy építése. Például 1973-ban a CIA számos nyílt és titkos akciót folytatott Chile-ben a chilei gazdaság működésének rombolásáért azzal a céllal, hogy társadalmi elégedetlenséget előidézve rávegyék a katonai vezetőket egy Salvador Allende elleni katonai puccs végrehajtására. A tervezett módszerek között

[25] Uo. p. 24.
[26] Uo. pp. 26-27.

szerepelt a munkások sztrájkra való bátorítása, illetve az erre hajlamot mutató csoportok anyagi támogatása.[27]

A CIA által végrehajtott fedett akciók 1948-ig, a csehszlovákiai kommunista puccsig, főleg a propaganda-akciók körébe tartoztak, ezt követően kerültek csak előtérbe a politikai akciók. Ugyan paramilitáris akció zajlott már 1949-től kezdve, ám az ilyen típusú, és a gazdasági akciók jellemzően 1950-től, a koreai háborútól kaptak nagyobb hangsúlyt.[28]

4. Magyarázati lehetőségek

Az iráni puccs magyarázatainak összessége igen összetett képet mutat, és számbavételükre, illetve közülük a jó magyarázat kiválasztására már a kezdetektől komoly kísérletek történtek.[29] A magyarázat kapcsán hagyományosan felmerülő kérdés arra vonatkozott, hogy ki vagy mi áll a puccs hátterében. A kérdésre válaszul a téma egyik kortárs vezető kutatója, Mark J. Gasiorowski a következő válaszlehetőségeket jelölte meg:

„*Moszadek követői általában külföldi erőket okolnak Moszadek bukásáért, úgy érvelve, hogy először a brit kormány és a nemzetközi olajvállalatok bojkottálták az iráni olajkereskedelmet, és folyamatosan konspirálva Moszadek ellen aláásták Moszadek hatalmát; ezt követően az Egyesült Államok a puccsal befejezte a munkát. A Moszadekkel szemben állók általában tagadják, hogy puccs történt volna, vagy hogy külföldi erők fontos szerepet játszottak volna az eseményekben, és ehelyett azzal érvelnek, hogy Moszadeket a nemzeti felkelés döntötte meg, amelyben az iráni nép felkelt a vezetője ellen, aki visszautasítva a megegyezést az olajvitában elfecsérelte népszerűségét, és diktatórikus eszközöket vett igénybe. Egy harmadik magyarázat, melyet az amerikai és a brit tisztviselők képviselnek, azt hangsúlyozza, hogy a külföldi erők tényleg szították a puccsot, azonban az ő lényeges hozzájárulásuk kizárólag abban állt, hogy bátorítsák az iráni erőket és asszisztáljanak nekik, akik így valójában a fő előidézői voltak Moszadek bukásának.*”[30]

Ez alapján a puccs lezajlásának lehetséges magyarázatait három nagy típusba sorolhatjuk: a puccsot vagy csak a külföldi erők hajtották végre, vagy csak a belföldi erők hajtották végre, vagy a belföldi erők a külföldiek valamilyen arányú segítségével.

Amennyiben a magyarázatban nem támaszkodunk a külföldiek segítségére, akkor az iráni nép spontán nemzeti felkelésére kell helyezni a hangsúlyt, amely Moszadek ellenében és Mohammed Reza Pahlavi sah érdekében zajlott le. A 60-as és a 70-es években voltak olyan akadémiai próbálkozások, amelyek ezt a magyarázatot részesítették előnyben.[31] Ennek a megközelítésnek az értékét azonban

---

[27] Uo. p. 26.
[28] Uo. pp. 101-102.
[29] RAHNEMA i. m. p. 9.
[30] GASIOROWSKI, Mark J.: Conclusion – Why Did Mossadeq Fall? In: Mark J. GASIOROWSKI – Malcolm BYRNE (eds): Mohammed Mosaddeq and the 1953 Coup in Iran; Syracuse, Syracuse University Press, 2004., p. 262.
[31] ABRAHAMIAN, Ervand: The 1953 Coup in Iran; In Science and Society (65); 2001., p. 211.

csökkenti, hogy maga sah is tulajdonított valamilyen szerepet a külföldi erőknek emlékirataiban és egyéb megnyilatkozásaiban;[32] illetve, hogy a 60-as és a 70-es években nem voltak nyilvánosak azok a források, amelyek ma már azok, sőt amelyek egy része már 1979-ben is nyilvánosságra került (például Roosevelt „Countercoup"-ja), és amelyek alapján egyértelmű a külföldi erők részvétele a puccsban. Továbbá, érdemes azt is megjegyezni, hogy a puccsot követően az USA teheráni nagykövete, Loy Henderson azt a taktikát javasolta az USA külügyminisztériumának, hogy indítsanak propaganda-kampányt, amiben hangsúlyozzák a puccs spontaneitását.[33] Úgy vélem tehát, hogy ezt a magyarázati lehetőséget elvethetjük.

Amennyiben a magyarázatban kizárólag a külföldi erők szerepét hangsúlyozzuk, akkor elsősorban a britek iráni szerepét kell szem előtt tartanunk, hiszen számukra a terület India védelmében a 19. század óta érdekszférának számított, a 20. század eleje óta pedig, az olaj megtalálásával, kiemelt érdekszférának. Számukra, legalábbis Moszadek hatalomra kerüléséig adott volt a lehetőség, hogy egymagukban befolyásolják az iráni belpolitikai történéseket. A puccsot azonban nem a britek hajtották végre, mégha közreműködtek is benne, hanem az USA Központi Hírszerzési Hivatala, amely pedig támaszkodott beszervezett és spontán módon összeállt polgári és katonai csoportok támogatására. Ennek megfelelően úgy vélem, hogy Gasiorowski második típusát is elvethetjük, azaz nem áll, hogy az 1953. augusztusi eseményeket kizárólag külföldi erők irányították volna. Ami ezek után marad a lehetőségek közül, az az, hogy az események irányítása és lezajlása egyaránt tulajdonítható külföldi és belföldi erőknek.

Ezzel az eredménnyel azonban csak részben lehetünk elégedettek, hiszen a magyarázat egy következő szintjén éppúgy kérdésessé lehet tenni azt, hogy milyen célok vezették a puccsban részt vállaló iráni erőket,[34] mint azt, hogy milyen célok vezették a puccsban részt vállaló külföldi erőket, Nagy-Britanniát[35] és az Egyesült Államokat. Ezen három kérdés megvizsgálása közül én egyre vállalkozom, az Egyesült Államok szerepének a megvilágítására. Ezzel a kérdéssel nem annyira arra keresem a választ, hogy összességében miként magyarázatható az iráni puccs megtörténte, hanem arra, hogy miként magyarázható az iráni puccshoz hozzájáruló CIA-művelet, a TPAJAX lezajlása.

Erre a kérdésre három válaszlehetőséget fogok megvizsgálni, amelyekből kettőt elvetek, és egy mellett érveket fogalmazok meg. Az első lehetséges magyarázat arra épít, hogy az iráni olaj nem csupán a britek számára bírt jelentőséggel, hanem az USA számára is, sőt az egész kapitalista világ számára. A magyarázat értelmében az USA a TPAJAX-ot az iráni olaj biztosítása érdekében hajtotta végre, hogy védje azt Moszadek erőszakos nacionalizáló politikájától.

---

32 RAHNEMA i. m. pp. 3-5.

33 Telegram of the Ambassador in Iran (Henderson) to the Department of State (Document 351.). In: FRUS, vol. X, pp. 759-760.

34 AZIMI, Fakhreddin: Unseating Mosaddeq: The Configuration and Role of Domestic Forces; In: GASIOROWSKI –BYRNE (eds) i. m.; BAYADOR, Darioush: Iran and the CIA, Basingstoke-New York, Palgrave Macmillan, 2010; és RAHNEMA i. m.

35 ROGER, Louis W.: Overthrow of the Mosaddeq Government; In: GASIOROWSKI – BYRNE (eds) i. m.

Ennek megfelelően a TPAJAX-ot offenzív fedett műveletnek kell tartani. A második lehetséges magyarázat szerint az USA célja a TPAJAX-szal a Tudeh párt által (és azon keresztül talán a Szovjetunió által is) egyre inkább támogatott Moszadek diktatórikus hatalomátvételének megakadályozása, majd az átvett hatalommal rendelkező Moszadek megtámadása és a hatalomból való kivetése volt. A TPAJAX ennyiben defenzív fedett akciónak tekinthető. Végül, a saját álláspontom szerint a TPAJAX-ot preventív akciónak kell tartanunk, mivel az USA célja az iráni nemzeti szabadság védelme volt a kommunista hatalomátvételtől olyan módon, hogy az események következményeképpen az USA gazdasági érdekei is kielégüljenek.

III. Az olaj: a demokratikus iráni nacionalizmus ellen

Az Iránban lévő amerikai olajérdekeltségekre hivatkozó magyarázat jelentős képviselője Ervand Abrahamian, aki a következőképpen foglalja a magyarázatot:

„*Az 1953-as puccs,..., az Irán és Nagy-Britannia között 1951-53 között fennálló krízisben gyökerezik. 1951 áprilisában az iráni parlament azzal a világos mandátummal választotta Moszadeket miniszterelnökké, hogy nacionalizálja a britek tulajdonában lévő Angol-Iráni Olajvállalatot. Ez indította el az „angol-iráni vita" néven elhíresült nemzetközi krízist. ... Az Egyesült Államok egy sor úgynevezett kompromisszumos megoldási javaslattal „becsületes közvetítőként" állította be a saját helyzetét, és ezzel igyekezett lehűteni a krízist. ...*
... Jelen könyv úgy érvel, hogy ez a kompromisszum elérhetetlen volt, mivel a vita valójában azon kérdés körül forgott, hogy „ki ellenőrizze az olajipart – az olaj feltárását, kitermelését, lepárlását, és exportját?". Az ellenőrzés Irán vagy az Angol-Iráni Olajvállalat kezében legyen, esetleg az akkoriban a Hét Testvér néven ismert nagy olajvállalatok alkotta konzorcium kezében? Irán számára a nacionalizáció szuverén ellenőrzést jelentett. Az olajvállalatok számára az iráni nacionalizáció az olaj nyugati ellenőrzésének az elvesztését jelentette, valami olyat, ami az 50-es évek elején elfogadhatatlan volt." [36]

Az olajérdekeltségekre építő magyarázatot alább Abrahamian: The Coup 1953, The CIA, and the Roots of Modern U.S.-Iranian Relations c. könyve alapján mutatom be és értékelem. A magyarázat elemzése során először nézzük az angol-iráni vitához vezető eseményeket, majd a kialakult helyzetet vessük össze az amerikai érdekekkel!

1. A brit érdekek

a. A brit érdekszféra kialakulása

A britek a 18. és a 19. század fordulóján nyomultak be India felől az akkor Perzsiának nevezett Iránba. A benyomulást követően a britek szerződésben támogatták a perzsákat az afgánokkal, az oroszokkal és a francia forradalmi és napóleoni befolyással szemben, cserébe pedig gazdasági jogosultságokat kértek és kaptak Perzsiában. A 19. században ezen jogosultságok keretében a briteké lett a

[36] ABRAHAMIAN, Ervand: The Coup 1953, The CIA, and the Roots of Modern U.S.-Iranian Relations, New York, The New Press, 2013., pp. 20-21.

vasút-, a bánya-, és a dohánykoncesszió, az állami bank felállításának joga, a távíró felállításának joga (megosztva a németekkel), és a számunkra kiemelkedő jelentőséggel rendelkező olajkoncesszió 1901-től.

1901-ben ugyanis William Know D'Arcy 60 évre 20.000 Ł-ért, ugyanakkora értékű vállalati részvényért és a jövőbeli profit 16%-áért megvásárolta a sahtól az Oroszországgal határos területeket, kivéve minden Perzsiában talált kőolajszármazék kutatásának, kitermelésének, finomításának és exportálásának jogát, és megalapította a D'Arcy Concession-t. Ugyan D'Arcy 1908-ban, a későbbi Huzisztánban olajat talált, a jogokat eladta a veszteséges Burmai Olajvállalatnak, amely 1909-ben felvette az Angol-Perzsa Olajvállalat (Anglo-Persian Oil Company – APOC) nevet (amely 1935-ben AIOC-ra (Angol-Iranian Oil Company) változott, azzal összhangban, hogy Perzsia felvette az Irán nevet). AZ APOC igazgatótanácsában a britek a szavazatok 52,5 %-ával rendelkeztek, illetve a társaság mindkét igazgatóját ők adták, az egyiket ráadásul a brit admiralitás. Az APOC bérbe vette a délnyugati törzsektől Ábádán szigetét, ahol olajfinomítót épített. Mivel a britek ebben az időszakban fejezték be a flotta átállítását a széntüzelésről olajtüzelésre (1913), ezért a perzsa olaj létfontosságú volt a brit állam számára, ami így 1914-ben felvásárolta a részvények 51%-át.[37]

A 1931-ben a gazdasági világválság következményeként ötödére esett vissza az az összeg, amit az APOC Perzsiának fizetett. Ennek következtében Perzsia újra kívánta tárgyalni a megállapodást. 1933-ban a tárgyalások eredménye az lett, hogy Perzsia ugyan garanciát kapott arra, hogy az őt megillető éves juttatás nem eshet egy bizonyos érték alá, azonban cserébe Perzsia vállalta, hogy egyoldalúan nem változtatja meg a koncessziós megállapodást, amelyet további 32 évvel meghosszabbítottak (1993-ig).

b. Moszadek és az olajüzlet nacionalizációja

Az iráni olajtartalék a világon a harmadik legnagyobb, a kitermelés a legnagyobb a régióban, és a negyedik legnagyobb a világon, az export pedig a második legjelentősebb a világon. Az ábádáni finomító a legnagyobb ilyen jellegű létesítmény volt a Földön akkoriban. A kitermelés és a kereskedelem folyamatos bővülése ellenére azonban Irán részesedése továbbra is a profit 20%-a körül maradt, annak ellenére, hogy a hasonló olajvállalatokban a világ más tájain az 50/50%-os profitosztozkodás volt az elfogadott (pl. Venezuela, Kuvait, Szaúd-Arábia, utóbbiak 1950-ben).[38] 1950-ben Irán 275 millió Ł-ot nyerhetett volna, ha ő birtokolja az iráni olajüzletet, az AIOC működésével azonban csak 37 millió Ł-ot nyert.[39]

Ezeknek a tényeknek a hatására is, 1947-ben Qavam iráni miniszterelnök tárgyalásokat kezdeményezett egy Irán számára kedvezőbb megállapodás tető alá hozásáról. A tárgyalások 1949-ig eltartottak, közben több miniszterelnök is vezette azokat, és 1949-ben a Kiegészítő Megegyezéssel (Supplementary Agreement-tel) zárultak le. Ez a megegyezés kiegészítette az 1933-as megállapodást, melynek értelmében tovább emelkedett az Irán számára juttatott összeg, ami azonban az 50-

[37] Uo. pp. 26-27.
[38] Uo. p. 30.
[39] McMurdo, Torey C.: The United States, Britain, and the hidden Justification of Operation AJAX In Studies in Intelligence (56), 2012., p. 16.

50%-os profitosztozkodástól még messze volt. A Kiegészítő Megegyezésnek továbbá a Parlament jóváhagyására is szüksége volt.

1951-ben egy fundamentalista iszlám szervezet, a Fedayan-e Islam „brit ügynöknek" nevezte a hatalmon lévő miniszterelnököt, Haj Ali Razmarát, és meggyilkolta.[40] Razmara volt az utolsó olyan politikus, aki kiállt a Parlamentben a Kiegészítő Megegyezés mellett. A Kiegészítő Megegyezés elfogadása az olaj nacionalizálásával szembeni kiállást is jelentette, a nacionalizálási terv azonban 1951-re komoly társadalmi támogatottságra tett szert. A támogatók között ekkor éppúgy megtalálhatók voltak az iráni politika vallásos szélsőjobboldali szereplői (például a Fedayan-e Islammal is kapcsolatban álló Kasáni[41]), mint később a puccsban fontos szerepet betöltő, szintén jobboldali katonai vezetők (például Záhedi tábornok). A nacionalizálás mellett kiálló politikai erők egyetlen lazább-szorosabb egységben tömörültek, a Nemzeti Frontban.

Moszadek is a Nemzeti Front teheráni listáján került be a Parlamentbe 1950-ben, majd nem sokkal később a frissen felállított, és az újabb brit koncessziót vizsgáló Parlamenti Olajbizottság (*Parliamentary Oil Committee*) elnöki székébe. Razmara meggyilkolásának másnapján Moszadek névnélküli szavazást tartott az Olajbizottságban, és ezzel párhuzamosan egy egyetlen cikkelyből álló törvényjavaslatot nyújtott be a Parlamentben az iráni olajüzlet nacionalizálásáról. A törvény így hangzott:
„*Az iráni nemzet boldogságáért és boldogulásáért, és a világbéke megőrzésének céljával, ezúton elhatározzuk, hogy az olajipart az ország minden részében, kivétel nélkül, nacionalizáljuk; ennek megfelelően minden olajfeltárást, lepárlást és hasznosítást csak a kormány hajthat végre.*"[42]

A Parlament március 14-én nagy többséggel elfogadta a törvényt.

A britek nem vették komolyan a törvényt, és a sah is olyan miniszterelnököt nevezett ki (Huszein Ala), aki igyekezett csillapítani a kedélyeket, ezért a Nemzeti Front képviselőit is kinevezte a kormányba, azonban nem törekedett a nacionalizálásra. Ennek következményeként általános sztrájk robbant ki az olajipari munkások között.

A sztrájknak csak április végén lett vége, amikor Ala lemondott, és Moszadek egy újabb, részletesebb – kilenc cikkelyből álló – törvény tervezetét nyújtotta be a Parlamentben. Ez a törvény létrehozott egy tizenkét főből álló bizottságot (Vegyes Bizottság), amelynek az első törvény megvalósításában szánt szerepet, az AIOC helyett létrehozta a Nemzeti Iráni Olajvállalatot (National Iranian Oil Company, NIOC), és a jövőbeli profit 25%-át ígérte a korábbi tulajdonosoknak kárpótlásul.[43] Ala lemondását követően a Parlament elnöke felajánlotta a miniszterelnöki széket Moszadeknek, amit Moszadek azzal a feltétellel fogadott el, hogy a Parlament megszavazza a kilenc cikkelyes törvényét is. A sah jelöltje a miniszterelnökségre Szajjid Zia lett volna, de akaratát Moszadek komoly támogatottsága miatt nem tudta keresztülvinni. Ennek megfelelően a sah május 1-jén aláírta a nacionalizációt kimondó kilenc cikkelyes törvényt.

---

40 ABRAHAMIAN (2013) i. m. p. 61.
41 Uo. p. 57.
42 Uo. p. 61.
43 Uo. p. 69.

c. Brit reakciók

A britek számára az olajüzlet nacionalizálása komoly gondot jelentett a jelentősen megváltozott világgazdasági környezetben. A második világháború kezdete óta ugyanis a megkötött Atlanti Charta és Bretton Woods-i szerződések, illetve a font sterling-övezet megszűnése miatt a világgazdaság alapvető pénzneme a font sterling helyett a dollár lett, ami komoly gazdasági veszteségeket okozott Nagy-Britanniának.[44] A világgazdaság új rendszerében a britek főként az iráni olajból származó bevételükből voltak képesek a háborús kölcsöneiket törleszteni, és gazdaságuk háborús működéséről békebeli működésre való visszaállítását megkezdeni.

Az AIOC és a britek ezért az olajüzlet feletti rendelkezési jogot mindenképpen meg kívánták tartani, amiért cserébe hajlandóak lettek volna 55/45%-os profitosztozkodást is elfogadni.[45] Moszadek számára azonban az olajüzlet feletti kontroll jelentette az állami szuverenitás, és a hidegháborúban való semlegesség biztosítékát.[46] Ezért Moszadek pontosan annyira ragaszkodott az olajüzlet feletti irányítás megszerzéséhez, mint amennyire a britek ragaszkodtak a megtartásához.

A britek egyszerre többféleképpen is igyekeztek megtartani/visszaszerezni a vállalatot, amennyiben tárgyalást kezdeményeztek Moszadekkel, megtámadták az iráni törvényt a hágai Nemzetközi Bíróság előtt, gazdasági szankciókat vezettek be Irán ellen, komolyan elgondolkodtak a nyílt katonai beavatkozáson, és saját fedett (SIS-) akciót indítottak azzal a céllal, hogy eltávolítsák Moszadeket a hatalomból.[47]

(i) <u>Tárgyalási kísérletek</u>[48]

A britek az olajkrízis időszaka alatt végig, folyamatosan kísérleteket tettek arra nézve, hogy tárgyalásos úton közvetlenül, vagy közvetítőn keresztül számukra kedvező eredményt érjenek el Iránnal. Az olajnacionalizálási törvény május 1-jei végrehajtását követően Nagy-Britannia azonnal jelezte Irán felé, hogy a törvénnyel Irán megszegte az 1933-as megállapodást, amelyben vállalta, hogy egyoldalúan nem változtatja meg a felek megegyezését. Ennek megfelelően az AIOC képviselői tárgyalást és harmadik fél döntőbíráskodását szerették volna. A britek által javasolt megegyezés alapja júniusban az 1933-as koncesszió volt, amelyet az AIOC-ot képviselő Basil Jackson még kiegészített azzal, hogy egyrészt az AIOC a tárgyalások alatt azonnal, egyszeri alkalommal fizet Iránnak 10 millió Ł-t, és havonta még 3 Ł-ot; másrészt pedig létrehoznak egy új, iráni tulajdonú vállalatot, amely az AIOC minden eszközének és üzletének a tulajdonosává válik. Ezek az engedmények azonban nem érintették volna a felügyeleti jogokat, amelyek továbbra is a briteknél maradtak volna. Moszadek azonban nem fogadta el ezt lehetőséget, és az amerikai elnök, Harry Truman közvetítését kérte.

---

44 McMURDO i. m. p. 16.
45 ABRAHAMIAN (2013) pp. 74-75.
46 Uo. p. 73., 82.
47 GASIOROWSKI Mark J.: The 1953 Cuop D'etat in Iran. In: International Journal of Middle East Studies (19), 1987., p. 263.
48 EBRAHIMI, Mansoureh: The British Role in Iran Domestic Politics (1951-1953), eBook, Springer, 2016, pp. 15-21.; ABRAHAMIAN (2013) i. m. pp. 89-104., 123-124.

A brit tárgyalási próbálkozást követően így júliusban egy amerikai tárgyalópartner igyekezett kiegyezni Iránnal, William Avarell Harriman. A tárgyalásokat követően azonban Moszadek csak arra tett ígéretet, hogy Irán hajlandó egyezkedni a britekkel, a nacionalizációs törvény (és nem az 1933-as megegyezés) alapján állva.

Az amerikai közvetítési kudarcot követően a britek ismét közvetlen tárgyalást javasoltak, ezúttal (augusztusban) Richard Stokes, a brit kormány *Lord Privy Seal*-je érkezett Teheránba. Stokes számára a legfontosabb szempont az volt, hogy az AIOC ne veszítse el korábbi vevőit, azaz hogy a kereskedelem zökkenőmentesen folyjék tovább. Ezen túl azonban ő sem engedett, hanem gyakorlatilag a Jackson-féle javaslatot porolta le azzal kiegészítve, hogy a profitot 50-50%-ban osztanák meg a felek. Moszadek most is elzárkózott a megegyezéstől.

A brit kormány a Stokes-féle tárgyalások sikertelensége után formális panaszt nyújtott be az ENSZ Biztonsági Tanácsánál (1951. október-november), aminek hatására a BT személyesen hallgatta meg Moszadeket New Yorkban. Moszadek érvelése annak megmutatására irányult, hogy a BT-nek nincs joghatósága az olajvitában, mivel az nem nemzetközi jogi probléma, hanem egy szuverén állam és egy privát társaság közötti nézeteltérés. Ez alapján Moszadek vádolta meg Nagy-Britanniát azzal, hogy az általa alkalmazott eszközökkel egy magánjellegű ügyből nemzetközi kérdést csinált. A BT szavazásán végül, mivel nem tudott megfelelő szavazatot gyűjteni, Nagy-Britannia képviselője is Moszadek mellett szavazott, amikor elfogadta azt a javaslatot, hogy a BT várja meg a Nemzetközi Bíróság ítéletét a kérdésben, és aztán tárgyalja újra a kérdést.

Az ENSZ BT meghallgatása után Moszadek Washingtonba utazott, ahol találkozott és tárgyalt Truman elnökkel. A kialakított amerikai álláspont szerint a NIOC megkapná a Kermánsáh-i finomítót, és felügyelné az összes olajmezőt, az ábádáni finomítót pedig eladná egy nem brit vállalatnak, amely iráni technikusokat képezne ki, illetve kölcsönözne Iránnak a saját szakemberei közül. A finomító ára az AIOC-hoz kerülne kompenzációként, amelyet a NIOC még megtoldana tizenöt évig évente 30 millió tonna finomítatlan kőolajjal. A NIOC vezetésében irániak (3 fő) és nem irániak (4 fő) is helyet kapnának, és a gazdálkodása alapvetően font sterlingben történne. Az amerikai javaslatot ugyan Moszadek hajlandó lett volna elfogadni, az újonnan megválasztott brit vezetés azonban nem.

Végül, „utolsó ajánlatként" a britek a Világbankon (Nemzetközi Bankon) keresztül tették meg ajánlatukat 1953 elején. Az ajánlat szerint a britek elismerik az olajüzlet nacionalizálását, cserébe a méltányos kompenzációért. A méltányos kompenzációt az AIOC az 1952-es éves profit alapján, és a koncesszió eredeti futamidejéből még hátralévő évek (1993-ig) számával felszorozva képzelte el. Az így számolt kompenzáció mértéke elérte a 100 millió Ł-os határt. Ezt a komoly mértékű kompenzációval járó megegyezést azonban Moszadek nem fogadta el (1953 márciusában), mivel az évtizedekre megkötötte volna Irán lehetőségeit. A tárgyalásos út ezzel zsákutcába került.[49]

[49] ABRAHAMIAN (2013) i. m. pp. 123-124.

(ii) A Nemzetközi Bíróság előtt

A tárgyalásos út mellett az ügyet Nagy-Britannia jogi úton is igyekezett döntésre vinni (1951. május – 1952. július). Nagy-Britannia a hágai Nemzetközi Bíróság előtt azzal érvelt, hogy Iránnak, mint szuverén államnak ugyan jogában áll a gazdaságának bármelyik részét nacionalizálni, azonban megsérti a nemzeti jog előírásait, ha – többek között – ezt egyoldalúan teszi (amit az 1933-as megegyezés tiltott), vagy cserébe nem ajánl méltányos kompenzációt, amelyet szintén szabályozott az 1933-as egyezség.[50] Irán ezzel szemben azzal az általános kifogással védekezett, hogy a Nemzetközi Bíróság joghatósága a kérdéses ügyre nem terjed ki, mivel a vita nem két szuverén állam között áll fenn, hanem egy szuverén állam és egy magánkézben lévő társaság között. Ugyanakkor Irán is elismerte, hogy méltányos kompenzációt kell fizetnie, azonban nem fogadta el, hogy a kompenzáció kiszámításának az alapja az 1933-as megállapodás legyen, mivel azt kikényszerített megállapodásnak tartotta. A Nemzetközi Bíróság 1952 júliusában hozott döntést, amelyben úgy határozott, hogy az ügy, az iráni érvelésnek megfelelően, nem tartozik a fennhatósága alá.[51]

(iii) Gazdasági szankciók

A britek a tárgyalásos és a jogi út mellett más módszerekkel is igyekeztek az iráni álláspont megváltozását elérni. Elsőként gazdasági szankciókat vezettek be Iránnal szemben, amelyekkel az olajkitermelés és olajkereskedelem ellehetetlenítését kívánták elérni. Lemondatták az olajüzletben dolgozókat, és igyekeztek elrettenteni az európaiakat attól, hogy az iráni olajüzletben dolgozzanak. Befagyasztották a londoni iráni bankszámlákat, továbbá mindenféle eszközzel igyekeztek eltéríteni a tankhajókat az iráni partoktól, és a diplomácia eszközeivel igyekeztek elérni, hogy harmadik fél ne vásároljon olajat Irántól.[52] Ennek hatására 1951 júliusára az iráni olajexport teljesen leállt, és a nagy olajvállalatok egy nemzetközi konzorcium keretében elosztották egymás között az AIOC korábbi ügyfeleit.[53]

(iv)Nyílt katonai akció

A gazdasági szankciók mellett a brit hadsereg is felkészült a nyílt támadásra, hogy a tengerről, illetve Irak területéről kiindulva védje a brit állampolgárokat, illetve foglalja el Ábádánt (MIDGET- és Buccaneer-hadművelet). A támadó jellegű hadműveleteket a brit miniszterelnök – amerikai kollégáikkal való egyetértésben, illetve általuk forszírozva – végül nem támogatta, ugyanis a koreai háború jellemezte feszült hidegháborús helyzetben a Szovjetunió észak-iráni beavatkozásától tartott.[54] A brit állampolgárok védelmében sem kellett defenzív jellegű erőszakot alkalmazni, mivel Nagy-Britannia felszólítására 1951. október elejére az utolsó brit állampolgár is elhagyta Iránt.[55]

---

50 Uo. p. 90.
51 Uo. p. 91.
52 Uo. pp. 91-92.
53 EBRAHIMI i. m. p. 29.
54 ABRAHAMIAN (2013) i. m. pp. 92-93.; EBRAHIMI i. m. pp. 23-24.
55 EBRAHIMI i. m. p. 25.

(v) Fedett akció

Nyílt katonai akció így nem indult Moszadek ellen, azonban a britek a Csizma-művelet (*Operation BOOT*) keretében többször is kísérletet tettek Moszadek eltávolítására úgy, hogy felhasználták a britekkel szimpatizáló politikusokat, katonai és vallási vezetőket, hogy nyomást gyakoroljanak az iráni sahra, illetve az iráni parlamentre, hogy velük szimpatizáló miniszterelnököt nevezzen ki.

Az első kísérletre 1951. júliusban került sor, amikor a britek lefizették többek között a Moszadek kormányában helyet foglaló, és a későbbiekben is fontos szerepet betöltő, Fezholláh Záhedi tábornokot, hogy a Nemzeti Front jobboldali tagjaival együtt tisztítsák meg a Nemzeti Frontot, és segítsék kormányra Záhedit. Záhedi korrumpálódása azonban Moszadek tudtára jutott, aki eltávolította Záhedit a kormányból.[56]

A következő puccskísérletekre a következő hónapokban került sor, hasonló forgatókönyv szerint. A britek a sahnál támogatták Szajjid Zia-t (1951-1952), Ahmad Qavam-ot (1952. július), majd az ismét aktivizálódó Záhedi tábornokot (1952. augusztus-szeptember), abban a reményben, hogy a sah kinevezi őket miniszterelnöknek. Bár Qavam kinevezésére, a többiekével ellentétben 1952. július 16-án sor került, miután a britek helyi ügynökeik segítségével képesek voltak megosztani a korábban teljesen Moszadek mögött álló Nemzeti Frontot, azonban a megélénkülő Moszadek-párti utcai tüntetéseknek köszönhetően (69 ember halt meg és 750 ember sérült meg) a kinevezés után néhány napon belül a sah menesztette Qavamot és ismét Moszadeket nevezte ki miniszterelnöknek.

A legutolsó ilyen jellegű puccskísérlet során Záhedi 1952. augusztus és szeptember során komoly támogatókat szerzett (amerikaiak, vallási vezetők – pl. Kasáni, törzsi vezetők – pl. Bahtijári). Szervezkedése azonban megint csak nem maradt titokban Moszadek előtt, aki októberben letartóztatási parancsot adott ki Záhedi ellen, aki azonban ekkor a Parlament tagja volt, ami mentességet biztosított számára. Moszadek ekkor már nemcsak az iráni szervezkedőkre csapott le, hanem október 16-án megszakította a diplomáciai kapcsolatait Nagy-Britanniával, és a brit diplomatákat kiutasította az országból.[57]

Nagy-Britanniának meg kellett szüntetnie iráni diplomáciai képviseletét, ami nem csak a helyzet nyomon követését nehezítette meg, hanem, mivel a puccsokat szervező SIS-ügynökök a legtöbbször diplomataként dolgoztak Teheránban, a fedett (SIS-) akciók további végrehajtását is. A britek Ciprusra, Nicosiába költöztették főhadiszállásukat és a segítség reményében 1952 őszén felvették a kapcsolatot a CIA-vel.

d. Az amerikai érdekek

A CIA és az Egyesült Államok végül átvállalta a britek helyett a cselekvő szerepet és sikeresen véghezvitte a puccsot. A kérdés, hogy az iráni térségben található olaj milyen vonatkozásban és milyen mélyen érdekelte az USA-t, hogy

[56] Uo. p. 19. 4. lábjegyzet
[57] GASIOROWSKI (1987) i. m. pp. 263-266.

annak biztosítása érdekében hajlandó volt komolyan beavatkozni Irán belpolitikájába.

Az Egyesült Államok gazdasági érdekei természetesen kapcsolódtak a korábbi és aktuális szövetséges Nagy-Britannia gazdasági érdekeihez.[58] A brit-iráni tárgyalási folyamatban azonban az USA igyekezett a semleges közvetítő szerepét felvenni, amely azt sugallja, hogy az USA legalábbis nem egyértelműen köteleződött el Nagy-Britannia nézőpontjának. Így a szövetségesi kapcsolat mellett szükség van olyan saját amerikai érdeknek a felmutatására is, amely jobban magyarázza az amerikaiaknak a puccsban betöltött szerepét.

Egy fontos amerikai érdek, amely ugyan saját érdek, azonban nem kizárólagosan amerikai, a nyugati-kapitalista világ komoly olajérdekeltsége. 1951-ban az amerikai Ministry of Fuel így figyelmeztette a politikai vezetést:
„*Moszadek elégedett lenne, ha azt látná, hogy az [olaj]ipar alacsony szinten termel a külföldi vezetés hiányában. Ez felvet egy problémát: a szabad világ biztonsága annak az olajnak a jelentős mennyiségétől függ, amely közel-keleti forrásokból származik. Amennyiben az iráni attitűd átterjedne Szaúd-Arábiára vagy Irakra, az egész rendszer romba dőlne, azzal a képességünkkel együtt, hogy megvédjük magunkat. Az alacsony termelési szint melletti olajvásárlás így veszélyes következmények lehetőségét hordozza magában.*”[59]

Az iráni olajüzlet nacionalizálása főként Nagy-Britannia számára jelentett gondot, azonban nem kizárólag, hanem komoly hatással volt általában véve a nyugati kultúrkör államaira is. Az 50-es években ugyanis az a közös meggyőződése volt a nyugati államoknak, hogy amennyiben Irán, vagy más, nem a nyugati kultúrkörbe tartozó állam teljesen nacionalizálná a területén az olajüzletet, akkor az a „civilizáció végét” jelentené, mivel a feltételezés szerint ezek az államok a nagyobb haszon érdekében nem bővítenék a kitermelést, hanem esetleg csökkentenék is, amivel azon nyomban komoly mértékben felvernék az olaj világpiaci árát.[60]

Végül az olajvita puccsot követő rendezése azt mutatja, hogy az amerikaiak a saját jogukon is érdekeltek voltak az iráni olajkészletekben.[61] Ha ugyanis megnézzük, hogy a puccsot követő időszakban Záhedi és a sah miként rendezte az olajvitát, akkor azt látjuk, hogy az olajüzlet nem került vissza sem a britek kizárólagos tulajdonába (az AIOC 25 millió $-os kárpótlást kapott), sem nem maradt Iránnál. Létrehoztak ugyanis egy konzorciumot, amely 50-50%-ban osztozott meg Iránnal (NIOC-cal) a profiton. A konzorciumon belül az AIOC jogutódja, a British Petrol 40%-s részvényhányaddal rendelkezett, ugyancsak 40%-ot kaptak az amerikai olajvállalatok, a holland Royal Dutch Shell 14%-ot, végül a francia Compagnie France pedig 6%-ot. A felügyeleti jogok ugyan Iránhoz kerültek, azonban a konzorcium 25 évre fenntartotta magának a jogot a kitermelés, a finomítás és a kereskedés ellenőrzésére.[62]

---

58 McMURDO i. m. p. 15.
59 ABRAHAMIAN (2011) i. m. p. 188.
60 ABRAHAMIAN (2013) i. m. pp. 73-74.
61 MARSH, Steve: Anglo-American Relations and Cold War Oil, Bolingstoke-New York, Palgrave Macmillan, 2003. pp. 163-168.
62 ABRAHAMIAN (2013) i. m. pp. 153-155.

IV. Az olajérdekekre építő magyarázat összegzése

A brit és iráni olajérdekek mentén körvonalazódó konfliktus a felszínen arról szólt, hogy ki, mennyit kapjon a kitermelt, finomított és értékesített olaj után. A konfliktus magja azonban sokkal inkább abban keresendő, hogy ki legyen az, aki felügyeli az iráni olajkészleteket és az iráni olajüzletet. Aki ugyanis birtokolja ezeket a felügyeleti jogokat, annak komoly politikai hatalma van a közel-keleti térségben, és komoly gazdasági-politikai hatalommal rendelkezik nemzetközi viszonylatban is. Úgy tűnik, hogy Moszadek, Nagy-Britannia és az Egyesült Államok egyaránt felismerte az olajvita jelentőségét ebben az utóbbi aspektusában is. Az olajvitát így azonban nem lehetett kompromisszumosan megoldani, hanem az nulla-összegű játszma volt, amelyben, ha az egyik fél nyer, akkor a másik veszít, vagy fordítva.[63]

Természetesen egyik fél sem kívánt veszíteni, ám az iráni fél nem rendelkezett azokkal az eszközökkel, amelyekkel a brit-amerikai fél igen. A brit „Csizma-művelet", és az abból kinőtt amerikai TPAJAX volt az a plusz tényező, amelynek a segítségével az olajvita végeredményben eldőlt, és a közel-keleti olajkincs, a nyugat olajellátottsága, illetve a világgazdaság továbbra is a nyugati nagyhatalmak, többek között az Egyesült Államok kezében maradt.

A tanulmány második része az iráni események két további magyarázatával foglalkozik, egy másik hagyományos magyarázattal, amely Irán korabeli kommunista fenyegetettségére épít, illetve az általam javasolt hibrid magyarázattal, amely szerint az események magyarázatában éppúgy jelentősége van a kommunista fenyegetésnek, mint az USA gazdasági érdekeinek.

Felhasznált irodalom:

- ABRAHAMIAN, Ervand: The 1953 Coup in Iran. Science and Society (65), 2011.
- ABRAHAMIAN, Ervand: The Coup 1953, The CIA, and the Roots of Modern U.S.-Iranian Relations, New York, The New Press, 2013.
- AZIMI, Fakhreddin: Unseating Mosaddeq: The Configuration and Role of Domestic Forces. In: Mark J. GASIOROWSKI – Malcolm BYRNE (eds): Mohammed Mosaddeq and the 1953 Coup in Iran, Syracuse, Syracuse University Press, 2004.
- BAYADOR, Darioush: Iran and the CIA, Basingstoke-New York, Palgrave Macmillan, 2010.
- CALLAHAN, James: Covert Action in the Cold War, London-New York, I.B. Tauris, 2010.
- DAVIES, Philip: MI6 and the Machinery of Syping; London and Portland (OR), Frank Cass, 2004.

[63] Uo. pp. 73-75.

- EBRAHIMI, Mansoureh: The British Role in Iran Domestic Politics (1951-1953), eBook, Springer, 2016.
- Final Report of the Select Commettee to Study Governmental Operations with Respect to Intelligence Activities, Washington, U.S. Government Printing Office, 1976.
- GASIOROWSKI, Mark J.: The 1953 Cuop D'etat in Iran. In International Journal of Middle East Studies (19), 1987.
- GASIOROWSKI, Mark J.: Conclusion – Why Did Mossadeq Fall? In: Mark J. GASIOROWSKI and Malcolm BYRNE (eds): Mohammed Mosaddeq and the 1953 Coup in Iran, Syracuse, Syracuse University Press, 2004.
- GASIOROWSKI, Mark J.: The CIA's TPBEDAMN Operation and the 1953 Coup in Iran. In Journal of Cold War Studies (15), 2013.
- JOHNSON, Loch K.: America's Secret Power, Oxford, OUP, 1989.
- LIGETI Lajos (szerk.): Keleti nevek magyar helyesírása, Budapest, Akadémiai Kiadó, 1981.
- LOUIS, W. Roger: Overthrow of the Mosaddeq Government. In Mark J. Gasiorowski and Malcolm Byrne (eds) Mohammed Mosaddeq and the 1953 Coup in Iran, Syracuse, Syracuse University Press, 2004.
- MARSH, Steve: Anglo-American Relations and Cold War Oil, Bolingstoke-New York, Palgrave Macmillan, 2003.
- MCMURDO, Torey C.: The United States, Britain, and the Hidden Justification of Operation AJAX. In Studies in Intelligence (56), 2012.
- NSC/4-A (Memorandum From the Executive Secretary (Souers) to the Members of the National Security Council), https://fas.org/irp/offdocs/nsc-hst/nsc-4.htm (Letöltés ideje: 2019. 02. 08).
- NSC 136/1. In FRUS 1952-1954, Iran, 1951-1954, United States Government Publishing Office Washington, 2017.
- Public Law 93 559-Dec. 30. 1974.
- Public Law 253, The National Security Act (1947).
- RAHNEMA, Ali: Behind the 1953 Coup in Iran, Cambridge, CUP, 2015.
- ROOSEVELT, Kim: Coutercoup, New York, McGraw-Hill Book Company, 1979.
- Telegram of the Ambassador in Iran (Henderson) to the Department of State (Document 351.). In FRUS, vol. X.
- WEINER, Tim: A CIA története, Budapest, GABO, 2009.
- WILFORD, Hugh: America's Great Game – The CIA's Secret Arabists and the Shaping of the Modern

FELEGYI JÚLIA

NEMZETKÖZI GYAKORLAT A MENEDÉKKÉRŐK SZEXUÁLIS IRÁNYULTSÁGÁNAK VIZSGÁLATA KÖRÉBEN

I. Bevezetés

Miért kell ezzel a kérdéskörrel foglalkoznunk? Mert a világ hetvenkét országában számít bűncselekménynek az azonos neműek közti szexuális kapcsolat, tizenháromban pedig halálbüntetés jár érte. A Genfi Egyezmény értelmében az aláíró államok a genfi öt ok fennállása esetén nem küldhetik vissza a származási országába a menedékkérőt. Az akkor még Bevándorlási és Állampolgársági Hivatalban általam vezetett menekültügyi meghallgatások tapasztalatai is ihlették a kutatást: egyre több és több afrikai menedékkérő hivatkozott menekülésének okaként homoszexualitásra. Az erre hivatkozó kérelmezők az esetek szenzitivitása és a nehezen bizonyíthatóság alapján számíthattak a kérelem pozitív elbírálására, mely nagyon sok esetben valótlan állításaikon alapult. Aktuális, hiszen idén született precedens értékű ítélet hazánk Bevándorlási és Menekültügyi Hivatala kontra nigériai kérelmező ügyben. Európában fokozott figyelmet kap minden, ami a migrációval van összefüggésben, így elég lehet akár egy helytelen, vagy megalapozatlan ítélet a témában, és az a globalizált világunkban nemzetközi botránnyá dagadhat.

Meglehet, az Európai Unióban Belgium az egyetlen olyan ország, amely közzéteszi a menedékkérelmek számát hivatkozási okonként, de a következő statisztikai adat jól mutatja, hogy nem lehet megkerülni a kérdéskört. 2008 és 2012 közötti menekültügyi határozatok száma összesen 67.576 darab volt, ebből 2992, azaz 4,43% a szexuális irányultságon vagy a nemi identitáson alapult. Világviszonylatban a Menedékjogi, Menekültügyi és Migrációs Szervezet (Organization for Refugee, Asylum & Migration - ORAM) becslése szerint évente valamivel kevesebb, mint 2500-an kapnak védelmet másságuk miatt.[1]

A genfi öt ok

A Genfi Egyezmény szerint menekült az, akit faji, illetve vallási okok, nemzeti hovatartozása, meghatározott társadalmi csoporthoz tartozása, illetve politikai meggyőződése miatti üldöztetése vagy az üldöztetéstől való megalapozott félelme miatt származási országán kívül tartózkodik, és nem tudja, vagy az üldöztetéstől való félelmében nem kívánja származási országa védelmét igénybe venni. Az üldöztetéstől való megalapozott félelem alapulhat olyan eseményeken is, amelyek

[1] GARTNER, Johannes Lukas: (In)credibly Queer: Sexuality-based Asylum in the European Union; https://www.humanityinaction.org/knowledgebase/578-in-credibly-queer-sexuality-based-asylum-in-the-european-union (Letöltés ideje: 2018. 09. 10.)

azután következtek be, hogy a külföldi származási országát elhagyta, vagy a külföldi olyan tevékenységén, amelyet a származási országa elhagyását követően fejtett ki.[2]

Meghatározott társadalmi csoport

Ennek minősül az üldöztetés szempontjából az emberek olyan csoportja, amelynek tagjai velük született jellemző tulajdonsággal vagy meg nem változtatható közös háttérrel rendelkeznek; esetleg az érintett országban egyértelműen elkülöníthető identitással rendelkeznek. Az üldözési okok közül ez a leginkább rugalmas fogalom, mely folyamatosan bővül. Ide tartoznak például a nemi identitás okán üldözöttek, a női nemiszerv-csonkítás áldozatai. Újabban a társadalmi nem (gender) okán üldözötteket is ide sorolják.

Meghatározott társadalmi csoporthoz tartozás lehet a gyökere az üldözésnek, ha nem hisznek egy csoport kormány iránti lojalitásában, vagy a csoport politikai szemléletmódja, tagjainak előélete, gazdasági tevékenysége miatt, illetőleg azért, mert a csoport létét, mint olyant, a kormánypolitika érvényesítését akadályozó tényezőnek tekintik. Pusztán a sajátos társadalmi csoporthoz tartozás általában nem elegendő a menekültstátusz megalapozásához. Ugyanakkor lehetnek olyan különleges körülmények, amelyek hatására önmagában e tagság elegendő alap lehet az üldöztetéstől való félelemhez.[3]

II. Magyar helyzetkép és precedens a 2018-as évben

Magyarországon a menekültügyi eljárás során a Bevándorlási és Menekültügyi Hivatal (továbbiakban BMH) meghallgatja a kérelmezőt, ahol annak be kell számolnia menekülése okairól, hazánkba érkezésének körülményeiről, valamint a kérelmét alátámasztó bizonyítékait a hatóságnak át kell adnia. Részleteznie kell, miért kényszerült hazája elhagyására, hogyan zajlott üldöztetése, pontosan mivel indokolja a beadott kérelmét, és mi akadályozza abban, hogy származási országába visszatérhessen. Lényeges, hogy hiánytalanul és a valóságnak megfelelően tárja fel menekülésének körülményeit, konkrétan nevezze meg a kérelmező az őt fenyegető veszélyt, mellyel hazatérése esetén számolnia kell. Az interjú alatt elhangzottakat ezt követően összevetik a származási országra vonatkozó aktuális, objektív országinformációkkal. Amennyiben az információk nem támasztják alá a meghallgatáson elhangzottakat, a kérelem elutasítható.[4] Meghallgatásaim során (főként a 2015-ös évben) egyre több és több Afrikából érkező menedékkérő hivatkozott arra, hogy homoszexualitása miatt üldöztetésnek volt kitéve, illetve hogy élete veszélyben forgott a származási országában. Ez felkeltette az érdeklődésemet, és a hazánkban legmagasabb létszámban menedéket kérő öt afrikai országot megvizsgáltam e szempontból is, melynek eredménye röviden összefoglalva az alábbi táblázatban olvasható.

---

[2] UNHCR: Convention and protocol relating to the status of refugees; http://www.unhcr.org/3b66c2aa10.html (Letöltés ideje: 2018. 09. 01.)

[3] Uo.

[4] Bevándorlási és Menekültügyi Hivatal: Tájékoztató a magyar menekültügyi eljárásról tömeges bevándorlás okozta válsághelyzet idején; http://www.bmbah.hu/index.php?option=com_k2&view=item&layout=item&id=1125&Itemid=1714&lang=hu# (Letöltés ideje: 2018. 09. 10.)

	Eritrea	Nigéria	Ghána	Gambia	Algéria
Faji, etnikai		X	X		
Vallási	X	X			X
Politikai	X			X	
Meghatározott társ. csoport	X	X	X	X	
Egyéb	szabadságjogok		igazságszolgáltatás		terrorizmus

Láthatjuk, hogy a meghatározott társadalmi csoporthoz való tartozás (esetünkben LGBTI valamely esete) az öt vizsgált országból négyben valós üldözési ok.

Idén év elején a C-473/16. sz. ügyben hozott ítélet „F" kontra Bevándorlási és Állampolgársági Hivatal ügyében, mely precedenst teremthetett az EU vonatkozásában a vizsgált kérdést tekintve.[5]

2015 áprilisában egy nigériai állampolgár menedékjog iránti kérelmet nyújtott be a magyar Bevándorlási és Állampolgársági Hivatalhoz, amelyben arra hivatkozott, hogy származása szerinti országában homoszexualitása miatt üldöztetésnek lenne kitéve. Ugyan a hatóságok megítélése szerint a kérelmező nyilatkozatai között nem voltak ellentmondások, elutasították a kérelmet, mert a kérelmező személyiségvizsgálata céljából kért pszichológus szakértői vélemény nem támasztotta alá a szexuális irányultságát. A nigériai állampolgár keresetet nyújtott be a határozat ellen a magyar hatóságokhoz, mert szerinte a szakértői vélemény pszichológiai tesztjei jelentősen sértik az alapvető jogait, valamint alkalmatlanok a szexuális irányultságának megállapítására.
Az ügyben eljáró Szegedi Közigazgatási és Munkaügyi Bíróság azt a kérdést tette fel az Európai Unió Bíróságának, hogy a magyar hatóságok vizsgálhatják-e a menedékkérő szexuális irányultságára vonatkozó nyilatkozatait pszichológus szakértői vélemény alapján. A Bíróság megállapította, hogy a menekült jogállás nyújtásának feltételeire vonatkozó irányelv lehetővé teszi a nemzeti hatóságok számára, hogy szakértői véleményt kérjenek a kérelmező nemzetközi védelem iránti valódi igényeinek pontosabb meghatározása céljából. A szakértői vélemény esetleges igénybevételére vonatkozó részletes szabályoknak azonban tekintettel kell lenniük az Európai Unió Alapjogi Chartájában biztosított alapvető jogokra, így az emberi méltóság tiszteletben tartásához való jogára, valamint a magán- és családi élet tiszteletben tartásához való jogokra.

Nem zárható tehát ki, hogy a menedékkérő szexuális irányultságával kapcsolatos nyilatkozatainak értékelésekor a szakértői vélemények bizonyos formái hasznosnak bizonyulnak a kérelemben előadott tények és körülmények értékelésekor, a Bíróság e tekintetben ugyanakkor kiemeli, hogy a kérelmező szexuális irányultságával kapcsolatos nyilatkozatainak értékelése során a nemzeti hatóságok és bíróságok **nem alapozhatják határozatukat kizárólag a szakértői vélemény következtetéseire.**

[5] Jogi Fórum: Tesztelhető-e a menedékkérő szexuális irányultsága? – Az Európai Unió Bírósága magyar vonatkozású ügyben hozott ítéletet; http://www.jogiforum.hu/hirek/38767 (Letöltés ideje: 2018. 09. 01.)

A Bíróság álláspontja alapján a menedékkérő szexuális irányultságának meghatározására irányuló pszichológiai szakvélemény elkészítése nem nélkülözhetetlen a kérelmező szexuális irányultságával kapcsolatos nyilatkozatai hitelességének értékeléséhez. A szakvéleménynek csak korlátozott a megbízhatósága, így a menedékkérő nyilatkozatai hitelességének értékelése során megkérdőjelezhető a hasznossága, főleg akkor, amikor – a mostani esethez hasonlóan – a kérelmező nyilatkozatai között nincsenek ellentmondások.
E körülmények között a Bíróság kimondta, hogy a Charta fényében értelmezett irányelvnek nem felel meg az, hogy pszichológus szakértői véleményt alkalmazzanak a menedékkérő szexuális irányultsága valódiságának értékeléséhez.[6] 2014-ben az uniós bírák hasonló döntést hoztak Hollandiában egy ügyről, ahol menedékjogot kapott a kérelmező homoszexualitása miatt.[7]

Érdemes arról is szót ejteni, hogy milyen pszichológiai vizsgálatok miatt fordult bírósághoz a felperes. A bírósági iratok alapján a kérelmezőnek egy embert kellett rajzolnia az esőben, szerepelt még a Rorschach-teszt, és a Szondi-teszt is. Azonban a magyar módszereknél jóval durvább teszteket is alkalmaztak már korábban más országokban, például a menedékkérő erekcióját vizsgálták, orvosi vizsgálatoknak vetették alá, vagy amint azt a briteknél említem, szexuális szokásaikról kérdezték őket. Utóbbiakról az EU Bírósága és a magyar bíróság is kimondta már, hogy tilosak. Tilos továbbá homoszexuális cselekmény végzését kérni a menedékkérőtől és erről készült videofelvétel sem fogadható el vagy kérhető bizonyítékként.[8]

III. Az Egyesült Királyság gyakorlatáról és szabályozásáról

Már a migrációs válságot megelőzően is felmerült a kérdéskör szabályozása a szigetországban. 2014 előtt a homoszexualitásukra hivatkozó menedékkérőknek meglehetősen intim és részletes kérdéseket tettek fel a menekültügyi meghallgatásuk során szexuális szokásaikról. Theresa May, akkori belügyminiszter asszony ezért felkérte a független határőrizeti és bevándorlási főfelügyelőt, John Vine-t, hogy vizsgálja felül a szexuális irányultság alapján történő menedékkérelmeket.[9]

2017. november 30-án jelentek meg az első hivatalos, de „kísérleti" statisztikák a szexuális üldöztetésre hivatkozó menedékkérőkről az Egyesült Királyságban. Ugyan a Home Office[10] felhívja a figyelmet a mintegy 12%-os hibahatárra, de egy megközelítő forrásként bátran tekinthetünk az adatsorra. A statisztika

---

6 Uo.

7 Telegraph: Tests to prove gay asylum seekers are telling the truth about their sexuality break EU law; https://www.telegraph.co.uk/news/2018/01/25/tests-prove-gay-asylum-seekers-telling-truth-sexuality-break/ (Letöltés ideje: 2018. 09. 02.)

8 KUGYELA Tamás: Hogyan döntsük el, hogy egy menedékkérő valóban homoszexuális? https://index.hu/kulfold/eurologus/2018/01/25/hogyan_dontsuk_el_hogy_egy_menedekkero_valoban_homoszexualis/ (Letöltés ideje: 2018. 09. 10.)

9 Telegraph: Review ordered into questioning over-intrusive questioning of gay asylum seekers, https://www.telegraph.co.uk/news/uknews/immigration/10730856/Review-ordered-into-questioning-over-intrusive-questioning-of-gay-asylum-seekers.html (Letöltés ideje: 2018. 09. 10.)

10 Home Office: a brit bevándorlási hivatal

megjelenésének hatására cikkek százai jelentek meg a melegjogi aktivisták tollából, védelmükbe véve az elutasított LGBTI-menedékkérőket. A statisztika közzétételét közel hat éves jogi huzavona előzte meg, ám végül a tavalyi év végén az alábbiak kerültek nyilvánosságra: a benyújtott menedékkérelmek közel 6%-a hivatkozik LGBT-csoporthoz való tartozás miatti üldöztetésre (az 58.761 kérelemből 3535), melynek mintegy 25%-a került támogatásra.[11] Érdekes adalék, hogy az elutasított pakisztáni kérelmezők fellebbezéseinek 39%-a zárult sikerrel.[12]

Írásbeli iránymutatást a meghallgatást végzőknek a Home Office „Asylum Policy instruction- sexual orientation in asylum claims" 2016-os kiadványa jelent. A dokumentum leszögezi, hogy az ilyen irányultságú kérelmező megválaszthatja a meghallgatáskor jelenlévő tolmács nemét is. Annak érdekében, hogy a kérelmező minden releváns, az ügyéhez tartozó információt átadhasson, a meghallgatónak a témával kapcsolatos kérdéseket kell feltennie. Például a kérelmező a származási országában járt-e ilyen jellegű klubokba, közösségbe, akár közösségi médiát használva tartotta-e a kapcsolatot ilyen érdeklődési körűekkel. A brit útmutató ugyanakkor felhívja a figyelmet, elképzelhető, hogy a kérelmező nem válaszol, vagy nem voltak ilyen jellegű kapcsolatai, és ez önmagában nem elég a kérelem elutasításához. A közismert találkozó helyek és tevékenységek, az LGBTI-csoportok figyelmen kívül hagyása nem feltétlenül jelzi a felperes hitelességének hiányát. A meghallgatást vezetőnek meg kell kérdeznie a kérelmező üldözésének körülményeit, hogy nemi identitása hogyan befolyásolta őt a származási országában és hogyan az Egyesült Királyságban. A meghallgatás során meg kell kérdezni, volt-e, illetve van-e azonos neművel kapcsolata, mely a bizonyítékok közt kerül majd értékelésre, ugyanakkor csak a fenti kérdésekre adott nemleges válasz nem elegendő ok az elutasításra. Abban az esetben, ha a kérelmező házas, esetleg már családos, mégis LGBTI-okokra hivatkozik, kérdéseket kell feltenni a házasságának körülményeiről, hátteréről. Következetes és ésszerű magyarázat esetén ezt figyelembe kell venni, mérlegelve a bizonyítékok hitelességét.[13]

A kérelmező szavahihetőségét erősíti, ha következetesen beszámol arról, hogy mikor és milyen körülmények közt észlelte magán az LGBTI-hez való vonzalmát. Nem szükséges továbbá, hogy a kérelmezőnek már legyen ilyen jellegű tapasztalata, kapcsolata, és bár ezek a tényezők jelentősek lehetnek, ezek nem meggyőzőek az egyén szexuális orientációját illetően. Amennyiben a kérelmezőnek van ilyen kapcsolata, az interjú során érdeklődni kell a szóban forgó kapcsolatok jellegéről. A döntéshozónak meg kell vizsgálnia minden benyújtott bizonyítékot, és össze kell vetnie az interjú során elhangzottakkal. Amennyiben a bizonyítékok, országinformáció, az interjú során elhangzott állítások között ellentmondások jelentkeznek, és a kérelmező nem tud ésszerű magyarázattal szolgálni, úgy az a kérelmező szavahihetőségét csökkenti. Ha nincs elegendő bizonyíték annak

---

[11] Az összes beadott menedékkérelem 31%-os támogatási aránya segítség lehet a viszonyításhoz.

[12] CHELVAN, S.: Comment: sexual orientation asylum statistics are good news; https://www.freemovement.org.uk/guest-post-sexual-orientation-asylum-statistics-are-good-news/ (Letöltés ideje: 2018. 09. 02.)

[13] Home Office: Asylum Policy instruction- sexual orientation in asylum claims; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/543882/Sexual-orientation-in-asylum-claims-v6.pdf (Letöltés ideje: 2018. 09. 11.)

megállapítására, hogy a kérelmező valamely LGBTI-csoporthoz tartozik, a kérelem elutasítható.[14]

2015-ben és 2016-ban „Difference, Stigma, Shame and Harm" (DSSH) címmel tartottak továbbképzést a homoszexuális menedékkérők kezelésével kapcsolatban a Home Office munkatársai részére.
Az Egyesült Királyság gyakorlata szerint a kérelmezőnek bizonyítania kell, hogy:

- meleg vagy homoszexuális
- olyan országból származik, ahol az LGBTI-csoport tagjainak megalapozott a félelme az üldöztetésektől. [15]

További segítség a tisztviselőknek, hogy tájékoztató és útmutató kiadványokat állított össze a témában az alábbi országok tekintetében: Nigéria, Pakisztán, Dél-Afrika, Srí Lanka, Törökország, Algéria, Gambia, Ghána, India, Irán, Jamaika, Kenya, Uganda, Ukrajna, Vietnam és Zimbabwe.[16]

IV. Az Amerikai Egyesült Államok eljárásrendje a kérdésre vonatkozóan

1990-ben, a Toboso-Alfonso-ügy volt az első a kontinens történetében, ahol a kubai Fidel Armando Toboso Alfonso homoszexualitására hivatkozva kért menedékjogot, és ezt a bíróság megtagadta. A bíró szerint ugyan jogilag jogosult volt a menedékjogra, viszont a kérelmező nem megfelelően támasztotta alá a származási országában meghatározott társadalmi csoporthoz való tartozását, és a homoszexualitás üldözésére sem szolgáltatott elegendő bizonyítékot.[17]

Az Egyesült Államok Bevándorlási Hivatala 2011-ben adta ki az „Útmutató a leszbikus, meleg, biszexuális, transzszexuális és interszexuális menekültek és menedékjog iránti kérelmek elbírálásához" kiadványát tisztviselői számára. A dokumentum egyértelmű definíciókkal szolgál a körülhatárolhatóságot elősegítendő.[18] A továbbképző kiadvány másik célja, hogy fokozzák a tudatosságot a szexuális kisebbségekkel szembeni problémákkal kapcsolatban, valamint következetes jogi és meghallgatási útmutatást nyújtsanak ezekkel a kérdésekkel kapcsolatban.

---

14 Uo. p. 12.

15 CHELVAN i. m.

16 European Migration Network: Ad-Hoc Query on NL AHQ on national asylum policies regarding LGBT-asylum seekers; https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/ad-hoc-queries-2016.1061_-_nl_ahq_on_national_asylum_policies_regarding_lgbt-asylum_seekers.pdf (Letöltés ideje: 2018. 09. 12.)

17 UNHCR: Matter of Toboso-Alfonso; http://www.refworld.org/cases,USA_BIA,3ae6b6b84.html (Letöltés ideje: 2018. 09. 01.)

18 U.S. Citizenship and Immigration Services: RAIO Directorate-Officer Training; https://www.uscis.gov/sites/default/files/USCIS/Humanitarian/Refugees%20%26%20Asylum/Asylum/Asylum%20Native%20Documents%20and%20Static%20Files/RAIO-Training-March-2012.pdf (Letöltés ideje: 2018. 09. 02.) pp. 12-13.

Meghatározott társadalmi csoporthoz való tartozás esetén a probléma elemzésénél a társadalmi láthatóságot vagy társadalmi különbséget is meg kell határoznunk, valamint azt, hogy mindez miben nyilvánul meg. Egyes döntéshozók tévesen úgy vélik, hogy a társadalmi láthatóság vagy megkülönböztetés megköveteli, hogy a kérelmező melegnek vagy homoszexuálisnak tűnjön. A valóságban inkább azt jelenti, hogy a szóban forgó társadalom megkülönbözteti azokat a személyeket, akik a fenti csoportokba tartoznak és elkülöníti azoktól, akik nem. A Hivatal szerint meghatározott társadalmi csoport tagjának tekinthetők:

a. Szexuális kisebbségek (pl. átalakító műtéten átesettek)
b. Meleg, leszbikus, transzszexuális vagy HIV-pozitív személyek
c. Üldöztetést szenved meleg, leszbikus, transzszexuális vagy HIV-pozitív volta miatt.

Bizonyítékként a menedékkérő vallomásából az alábbiak fogadhatóak el:
- amit az üldöző mondott vagy tett a kérelmezőnek,
- az üldözés aktusának összefüggése (például ha a kérelmezőt megtámadták egy bárban, mert egy vele azonos nemű kezét fogta),
- megbízható országinformáció, amely alátámasztja az ilyen bizonyságot.[19]

A politicalasylumusa.com LGBTI-kérelmezők számára az alábbi információkkal szolgál:
A politikai menedékjog megszerzésének egyik kulcskritériuma, hogy az LGBTI-csoporthoz való tartozás valós; a másik pedig, hogy bizonyítást nyerjen az egyén kezelése az LGBTI-identitás miatt üldöztetésnek számít származási országában.

Láthatóság

A láthatóság nem jelenti azt, hogy valaki úgy néz ki, mintha ezen csoportba tartozna. Általában elegendő, ha a hatóság bármilyen megkülönböztető magatartást lát. Csak azért, mert egy országnak nincs korábbi LGBTI-menedékjog iránti kérelme, nem jelenti azt, hogy a jövőben sem fog érkezni. Azonban egy LGBTI-menekültnek ebben az esetben elegendő bizonyítékot kell biztosítania annak bizonyítására, hogy kormánya diszkriminatív magatartást tanúsít az ilyen helyzetben lévőkkel szemben, azaz a genfi öt ok általi fenyegetés fennáll.

Üldözés

Amellett, hogy bemutatja, hogy a származási ország diszkriminálja az LGBTI-csoporthoz tartozó embereket, a menedékkérőnek a szexuális irányultsága vagy identitása miatti üldöztetést is bizonyítania kell. Ha egy országban bűncselekmény az LGBTI-csoport tagjai közti szexuális cselekmény, akkor az üldözés bizonyított.[20]

[19] Uo. p. 15.
;[20] Political Asylum USA: LGBTI; https://www.politicalasylumusa.com/application-for-asylum/gay-lgbt/ (Letöltés ideje: 2018. 09. 01.)

V. Az EU gyakorlata

Bár az EU tagállamokat az e csoportba tartozó menedékkérelmek kezelésére vonatkozó közös előírások vezérlik, a nemzeti szintű politikák eltérhetnek. Egy 2016-os, az European Migration Network által készített felmérés[21] szerint a tagállamok az alábbi gyakorlatokat alkalmazzák a szexuális irányultságú esetek interjúja és értékelések során:

- Figyelembe kell venni a menedékkérőnek a felelős tisztviselő és tolmács nemére vonatkozó preferenciáját (**Németország**);
- Orvosi és/vagy pszichológus szakértői véleménykérés *lehetősége* (**Magyarország**);
- A szexuális irányultság és a nemi alapú állítások feldolgozása egy speciális egységgel (**Belgium**) vagy LGBT-szakértővel (**Svédország**);
- Speciális képzés a menekültügyi kérdéseket illetően a szexuális orientációról a tolmácsok számára (**Belgium**);
- Ha lehetséges, a menedékkérő partnerével folytatott megbeszélés (**Cseh Köztársaság**).

Ami a származási országokat illeti, **Belgium** megkülönbözteti azon származási országokat, ahol a homoszexuálisok sebezhető csoportot jelentenek (például Kamerun, Irán, Irak). **Németország** speciális LGBTI-országinformációval rendelkezik Egyiptomról, Etiópiáról, Afganisztánról, Albániáról, Algériáról, Örményországról, Bangladesről, Görögországról, Guineáról, Indiáról, Irakról, Iránról, Koszovóról, Marokkóról, Macedóniáról, Montenegróról, Nigériáról, Oroszországról, Szerbiáról, Srí Lankáról, Szudánról, Dél-Szudánról, Törökországról, Tunéziáról és Ukrajnáról. **Hollandia** a származási ország helyzetét értékeli a kormánytól származó hivatalos jelentések és más, megbízható NGO-jelentések alapján. **Norvégia** országspecifikus jegyzeteket készít a fő származási országokkal kapcsolatos gyakorlatról, beleértve a szexuális irányultsággal kapcsolatos kérdéseket (pl. Etiópia, Nigéria, Irán és Pakisztán esetén).

A felmérés[22] azt a kérdést is vizsgálta, hogy az egyes tagországok milyen irányelvek mentén haladnak egy LGBTI-kérelmezővel kapcsolatos interjú és a döntéshozatal kapcsán. Közel sem minden ország válaszolta meg a feltett kérdéseket, így a válaszok közül a hasznosabbak, gyakorlatiasabbak közül ismertetnék párat.

Belgium az Egyesült Nemzetek Menekültügyi Főbiztosságának iránymutatásait alkalmazza. A belga tisztviselők rendelkeznek külön belső irányelvvel. Ez az irányelv tulajdonképpen egy függelék, mely a menedékkérő szexuális orientációjának hitelességét értékeli. Az irányelv bemutatja azokat az elméleti szempontokat, amelyek szükségesek ahhoz, hogy jobban megértsük a menekültet, valamint gyakorlati és konkrét utasításokat tartalmaz a menedékkérővel

---

[21] European Migration Network: Ad-Hoc Query on NL AHQ on national asylum policies regarding LGBT-asylum seekers; https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/ad-hoc-queries-2016.1061_-_nl_ahq_on_national_asylum_policies_regarding_lgbt-asylum_seekers.pdf (Letöltés ideje: 2018. 09. 12.)

[22] Uo.

és a döntéshozatallal kapcsolatban. A függelék segít a tisztviselőknek, hogy megfogalmazzák véleményüket arról, hogy a menedékkérő valóban homo(bi)szexuális vagy nem. Ezen változók közé tartozik többek között a menedékkérő tájékozottsága a homoszexualitásról, személyes életútja – e szexuális irányultság figyelembevételével – gyermekkorától kezdve, homoszexuális tapasztalatok stb. **Horvátország** a klasszikus menekültügyi eljárást alkalmazza, kiegészítve azzal, hogy ha a kérelmező LGBTI-okokra hivatkozik, megvizsgálják szavahihetőségét, a származási ország országinformációjával összevetik, és amennyiben valóban veszély fenyegeti a kérelmezőt, védelmet kap. **Finnország** is hasonlóképp jár el, kiegészítve a DSSH (Difference, Shame, Stigma, Harm) modellel. **Málta** hangsúlyozza, hogy esetükben igen minimális az ilyen jellegű kérelmek száma, de kurzusokon foglalkoztak a bevándorlási tisztviselők a kérdéssel. A szigetországban nem alkalmaznak orvosi szakértőt ilyen esetekben, ahogy provokatív kérdéseket sem tesznek fel, és semmilyen szexuális cselekményt nem fogadnak el bizonyítéknak; ahogy **Hollandia** sem. Érdekesség, hogy **Szlovákia** viszont megemlíti az interjú és országinformáció mellett az orvosi vizsgálat lehetőségét is. **Svédország** a standard eljáráson kívül, amennyiben LGBTI-ügyfélről van szó, kirendel az ügyben egy LGBTI-szakértőt is, aki minden, az üggyel kapcsolatos cselekménynél jelen lehet.[23]

VI. Összegzés, következtetések

Az idén hozott Európai Unió Bíróság ítéletét követően hazánk lehetőségei az LGBTI-okokra hivatkozó menedékkérőkkel kapcsolatban csökkentek is, meg nem is. Ugyan nem fogadható el egy pszichológusi szakvéleményre alapozott döntés a vizsgált kérdéskörben, de megalapozott igény esetén továbbra is segítheti a döntéshozatalt. A strasbourgi ítélet ismét fókuszba helyezte a menekültkérelmek ezen érzékeny kérdéskörét, és ugyan statisztikai adatokkal nem tudom alátámasztani, de gyakorlati tapasztalataim alapján úgy gondolom, növekedni fog az ilyen jellegű kérelmek száma. Ennek két oka lehet: egyrészt elképzelhető, hogy több, LGBTI-csoportba tartozó kérelmező érkezik harmadik országból az EU területére, esetleg egyszerűen csak mostanában merik felvállalni azt, hogy ilyen okokból kényszerültek menekülni. Másrészt meg kell említenem azt az eshetőséget is, hogy ismerve az európai hozzáállást az emberi jogok tiszteletben tartásáról és tudva, hogy az LGBTI-kérdéskör szabályozása nincs kiforrva, egyre több menedékkérő fog ilyen jellegű okokra hivatkozni, anélkül hogy ezek fennállnának.
Legyen szó bármelyik, vagy mindkét esetről, mind hazai, mind nemzetközi szinten szükségesnek tartom, hogy a meghallgatásokat végző és a döntéshozó szakembereink felkészültebbek legyenek az ilyen esetekre, és ahogy több ország példáján keresztül láthattuk, számos lehetőséget meg kellene fontolni, hogy alkalmazzon a magyar hatóság. Ugyan a BMH rendelkezik országinformációval, ugyanakkor nem tudok aktuális, naprakész LGBTI-specifikus jelentésekről, melyek ilyen esetekben jelentősen megkönnyíthetnék a döntéshozó munkáját. Hasznosnak gondolnám egy lista létrehozását is, melyen az LGBTI-veszélyeztetett országok szerepelnek a német és belga mintához hasonlóan. A szakemberek továbbképzése mindig és mindenkor megtérül, nem csak LGBTI-specifikus témaköröket érintenek

[23] Uo.

ezeken. Több, alapvető bizonyítékok értékelése, meghallgatási és tolmácskezelési technika, valamint pszichológia is hasznosnak bizonyulhat.

A 2015-ös számokhoz képest jelentősen kevesebb hazánkban a menedékkérők száma, egy újabb krízishelyzet azonban bármikor bekövetkezhet, és fontosnak tartom kihasználni arra az időt, hogy elemezzük, értékeljük a környezetünket és felkészüljünk a menedékkérelmek szakszerű és naprakész kezelésére.

Felhasznált irodalom:

- Bevándorlási és Menekültügyi Hivatal: Tájékoztató a magyar menekültügyi eljárásról tömeges bevándorlás okozta válsághelyzet idején; http://www.bmbah.hu/index.php?option=com_k2&view=item&layout=item&id=1125&Itemid=1714&lang=hu# (Letöltés ideje: 2018. 09. 10.)
- CHELVAN, S.: Comment: sexual orientation asylum statistics are good news; https://www.freemovement.org.uk/guest-post-sexual-orientation-asylum-statistics-are-good-news/ (Letöltés ideje: 2018. 09. 02.)
- European Migration Network: Ad-Hoc Query on NL AHQ on national asylum policies regarding LGBT-asylum seekers; https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/ad-hoc-queries-2016.1061_-_nl_ahq_on_national_asylum_policies_regarding_lgbt-asylum_seekers.pdf (Letöltés ideje: 2018. 09. 12.)
- GARTNER, Johannes Lukas: (In)credibly Queer: Sexuality-based Asylum in the European Union; https://www.humanityinaction.org/knowledgebase/578-in-credibly-queer-sexuality-based-asylum-in-the-european-union (Letöltés ideje: 2018. 09. 10.)
- Home Office: Asylum Policy instruction- sexual orientation in asylum claims; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/543882/Sexual-orientation-in-asylum-claims-v6.pdf (Letöltés ideje: 2018. 09. 11.)
- Jogi Fórum: Tesztelhető-e a menedékkérő szexuális irányultsága? - Az Európai Unió Bírósága magyar vonatkozású ügyben hozott ítéletet; http://www.jogiforum.hu/hirek/38767 (Letöltés ideje: 2018. 09. 01.)
- KUGYELA Tamás: Hogyan döntsük el, hogy egy menedékkérő valóban homoszexuális? https://index.hu/kulfold/eurologus/2018/01/25/hogyan_dontsuk_el_hogy_egy_menedekkero_valoban_homoszexualis/ (Letöltés ideje: 2018. 09. 10.)
- Political Asylum USA: LGBT; https://www.politicalasylumusa.com/application-for-asylum/gay-lgbt/ (Letöltés ideje: 2018. 09. 01.)

- Telegraph: Review ordered into questioning over-intrusive questioning of gay asylum seekers; https://www.telegraph.co.uk/news/uknews/immigration/10730856/Review-ordered-into-questioning-over-intrusive-questioning-of-gay-asylum-seekers.html (Letöltés ideje: 2018. 09. 10.)
- Telegraph: Tests to prove gay asylum seekers are telling the truth about their sexuality break EU law. https://www.telegraph.co.uk/news/2018/01/25/tests-prove-gay-asylum-seekers-telling-truth-sexuality-break/ (Letöltés ideje: 2018. 09. 02.)
- UNHCR: Convention and protocol relating to the status of refugees; http://www.unhcr.org/3b66c2aa10.html (Letöltés ideje: 2018. 09. 01.)
- UNHCR: Matter of Toboso-Alfonso; http://www.refworld.org/cases,USA_BIA,3ae6b6b84.html (Letöltés ideje: 2018. 09. 01.)
- U.S. Citizenship and Immigration Services: RAIO Directorate-Officer Training; https://www.uscis.gov/sites/default/files/USCIS/Humanitarian/Refugees%20%26%20Asylum/Asylum/Asylum%20Native%20Documents%20and%20Static%20Files/RAIO-Training-March-2012.pdf (Letöltés ideje: 2018. 09. 02.)

DR. RÉPÁSI KRISZTIÁN

AZ EURÓPAI UNIÓ LAKOSAINAK TERRORIZMUSSAL KAPCSOLATOS FENYEGETETTSÉG-PERCEPCIÓJA 2012 TAVASZA ÉS 2018 TAVASZA KÖZÖTT

Egy ország terrorfenyegetettségét elsősorban olyan tényszerűnek és objektívnek tekinthető adatok mutatják meg, mint a merényletek, a letartóztatások és a bírósági ítéletek száma, illetve az országban működő terrorista szervezetek aktivitása. Mindezek mellett azonban szükséges megvizsgálni azt is, hogy mi az ott élő emberek – szubjektívnek mondható – véleménye a terrorizmusról és a terrorfenyegetettségről. Az Európai Unió lakosságának fenyegetettség-percepcióját azért fontos elemzés tárgyává tenni, mert a vizsgálat megmutatja, hogy az EU polgárai miként érzékelik a terrorfenyegetettséget, illetve, hogy mennyire tartják a mindennapi életüket meghatározó tényezőnek a terrorizmust. Ezenfelül a felmérések eredményei azért is lehetnek fontosak, mi több tanulságosak, mert az Unió lakosainak terrorizmussal kapcsolatos elképzelését, véleményét már egy jó ideje számos tényező próbálja befolyásolni. Ezek közé sorolható többek között:

- A magas áldozatszámmal és nagy médiafigyelemmel járó, valamint a lakosság körében általános félelmet kiváltó stratégiai jelentőségűnek mondható terrortámadások.
- A tény, hogy 2015 és 2018 között az EU-ban végrehajtott négy stratégiai jelentőségű terrortámadásból[1] mind a négy vallási indíttatású volt. Ez idő alatt hiába hajtottak végre az Unióban többször annyi szélsőbaloldali és szeparatista terrorcselekményt, illetve szélsőjobboldali támadást, a legtöbb esetben a halálos áldozatok maximalizálására történő kísérletek miatt a szélsőséges muszlimok által végrehajtott akciók hagytak mélyebb nyomot az emberekben.
- Az elmúlt közel két évtizedben világszerte elkövetett stratégiai jelentőségű terrortámadásokat jórészt muzulmánok követték el (a 2001. szeptember 11-i New York-i és washingtoni merényletsorozatot, a mumbai terrortámadást, a beszlani vérengzést stb.).
- A 2001. szeptember 11-e után meghirdetett terrorizmus elleni harc elsősorban a vallási indíttatású és ezen belül is az iszlamista szélsőségeseket célozta meg, míg a terrorizmus többi válfajának képviselői jóval kisebb figyelmet kaptak.
- A terrorizmus elleni harccal összefüggésben nagyon sok esetben a fegyveres ellenállók által végrehajtott akciók is terrorcselekményként szerepelnek a hírekben, maguk a felkelők pedig általában terroristaként, figyelmen kívül hagyva, hogy nem minden fegyveres támadás számít terrorcselekménynek és nem minden lázadó szervezet tekinthető terrorista szervezetnek.
- A média és a politikai kommunikáció túlhangsúlyozzák a terrorizmus problémáját, végső soron azt sugallva, hogy a terrorizmus az egyik legnagyobb veszély az Európai Unióra nézve, a vallási indíttatású terrorizmust pedig úgy

[1] A 2015. januári és novemberi Párizsban végrehajtott támadások, a 2016. márciusi brüsszeli merényletsorozat és a 2016. július 14-i nizzai terrortámadás.

pozícionálják, mintha a terrorizmusnak ez lenne az egyedüli, kizárólagos típusa.

Az Eurobarometer az „EU egyik legrégebben használt, standardizált, összeurópai közvélemény-kutatása. 1973 óta készítenek ilyen felméréseket, amelyek időről-időre felmérik a tagállamok lakosságának véleményét, elképzeléseit az EU-val mint közösséggel, valamint különböző jelenségekkel kapcsolatban".[2] Az Eurobarometer egyik nagy csoportját az úgynevezett Standard Eurobarometer alkotja, *„amely az EU lakosainak véleményét méri fel az EU legfontosabb kérdéseivel kapcsolatban félévi rendszerességgel, előre kidolgozott módszertan alapján, gyakorlatilag ugyanolyan kérdésekkel harminc éve. Ezekből a jelentésekből kiderül, hogy mit gondolnak az egyes országokban az EU aktuális helyzetéről, mit várnak az uniós intézményektől, mennyire bíznak bennük, milyen vívmányokkal vagy nehézségekkel azonosítják az EU-t"*.[3]

A fentiekből kiindulva megvizsgáltuk, hogy az Eurobarometer (Standard Eurobarometer) felmérései szerint 2012 tavasza és 2018 tavasza között[4] a megkérdezettek miként vélekedtek a terrorizmusról, azaz mennyire tartották fontosnak a személyes életükre, országukra és az Európai Unióra nézve a terrorizmust.[5]

A terrorizmustól való félelem felerősödése 2015-öt követően

Az Eurobarometer felméréseinél a kérdéssorban felsorolt 13-15 probléma közül a válaszadók a nemzeti (országos) szintű kihívásokkal kapcsolatosan 2012 és 2015 között a terrorizmust többször is az utolsó helyre tették, vagyis százalékban kifejezve általában véve a megkérdezettek kevesebb, mint 7%-a helyezte a terrorizmust a nemzeti szinten megjelenő két legfontosabb probléma közé. A helyzet 2015 őszén változott meg jól érzékelhetően,[6] amikor a terrorizmus a 13 kérdésből a fontossági sorrendben a tizenharmadik (utolsó) helyről a hatodik helyre került, vagyis a válaszadók 11%-a gondolta úgy, hogy a terrorizmus a lényegesnek tekinthető országos szintű kérdések közé tartozik. A terrorizmus 2016 tavaszán a

---

2 Eurobarometer – az európai lakmusz; Európa Pont, 2013. 03. 29. http://europapont.blog.hu/2013/03/29/eurobarometer (Letöltés ideje: 2018. 11. 25.).

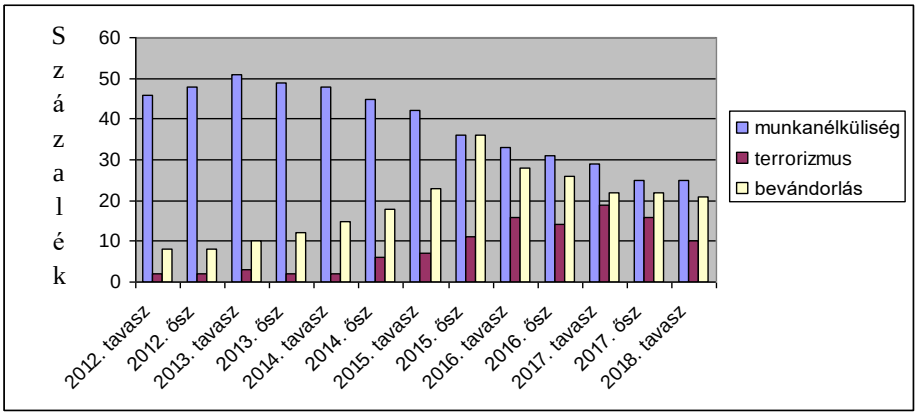
3 Uo.

4 Azért 2012-vel kezdtük a vizsgálatot, mert érzékeltetni akartuk, hogy évekkel a fentebb említett, „európai mércével" mérve számos halálos áldozattal járó merényletek előtt, illetve a 2015-ös menekült- és bevándorlási hullámot megelőzően mennyire féltek az EU lakosai a terrorizmustól. Jelen sorok írásakor a 2018-as őszi felmérés adatai csak részben voltak elérhetőek, ezért a szöveg koherenciáját szem előtt tartva vizsgálatunkat a 2018 tavaszán végzett felmérés elemzésével zártuk.

5 A kérdezők egész pontosan arra voltak kíváncsiak, hogy mi a két legfontosabb kérdés vagy probléma, amivel egyéni, nemzeti, illetve uniós szinten foglalkozni kell (And personally, what are the two most important issues you are facing at the moment?; What do you think are the two most important issues facing [OUR COUNTRY] at the moment?; What do you think are the two most important issues facing the EU at the moment?).

6 Valójában már 2014 őszén tapasztalható volt némi változás a korábbi felmérési eredményekhez képest, vagyis egész pontosan 2014 őszétől datálható, hogy a nemzeti szinten megjelenő problémákkal kapcsolatosan a terrorizmus egyre fontosabbá vált a közvélemény szemében.

fontossági sorrendben még előrébb – a negyedik helyre (16%) – lépett. A 2016-os őszi felmérés idején ugyan visszacsúszott a hetedik helyre, de a 2017-es tavaszi felmérésnél ismét a negyedik legfontosabb kérdésként jelent meg a válaszadók körében (19%). Ezt követően azonban a terrorizmus vesztett a fontosságából és 2018 tavaszán a 10. helyre csúszott vissza (10%).



1. ábra: A nemzeti szinten megjelenő problémák közül a terrorizmustól való félelem alakulása összevetve a munkanélküliségtől és a bevándorlástól való félelemmel 2012 tavasza és 2018 tavasza között

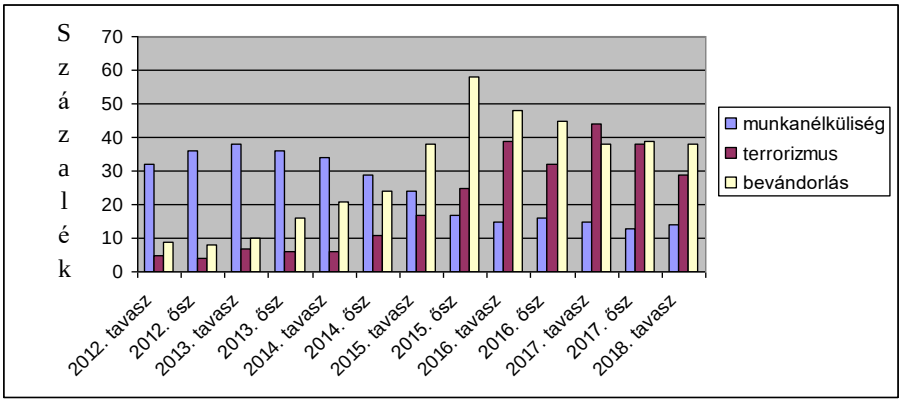
Forrás: Standard Eurobarometer 77-89. Készítette a szerző.

2. ábra: A válaszadók által a hat legtöbbet említett országos szinten megjelenő kihívás. A legfontosabb nemzeti szinten kezelendő problémák közé a korábbi felmérésektől eltérően 2018 tavaszán nem került be a terrorizmus.

Forrás: Standard Eurobarometer 89, Spring 2018, p. 20.

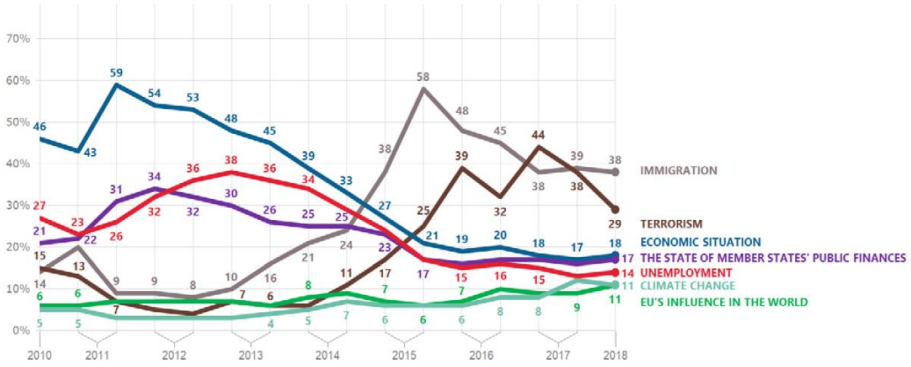
Az Európai Unió szintjén megjelenő legfontosabb kérdéseket illetően 2014 őszéig hasonló képet kapunk: 2012 tavasza és 2014 ősze között a válaszadóknak átlagosan mindössze 6%-a gondolta úgy, hogy az Uniót érintő legfontosabb problémák közé tartozik a terrorizmus, ami azt jelenti, hogy a fontossági sorrendben a 13 probléma közül hol a hatodik, hol a nyolcadik, hol pedig a kilencedik-tizedik helyre került. 2014 őszétől kezdve azonban ezen a téren is emelkedés, mi több, meredek emelkedés volt tapasztalható: a 2015. őszi felmérés során a megkérdezetteknek már 25%-a gondolta úgy, hogy a terrorizmus az EU lényeges

problémái között tartandó számon, előreléptetve a fontossági sorrendben a második helyre. Ezt a pozíciót a következő két felmérés során is megőrizte, s 2015 őszéhez képest százalékosan is nőtt azok aránya, akik a terrorizmust az EU-t érintő legfontosabb kérdések közé sorolták,[7] olyannyira, hogy 2017 tavaszán a terrorizmus átvette a vezetést a bevándorlástól a fontossági sorrendben. Ezt követően 2017 őszén és 2018 tavaszán a terrorizmus visszaszorult a második helyre a bevándorlás mögé.



3. ábra: Az uniós szinten megjelenő problémák közül a terrorizmustól való félelem alakulása összevetve a munkanélküliségtől és a bevándorlástól való félelemmel 2012 tavasza és 2018 tavasza között

Forrás: Standard Eurobarometer 77-89. Készítette a szerző.

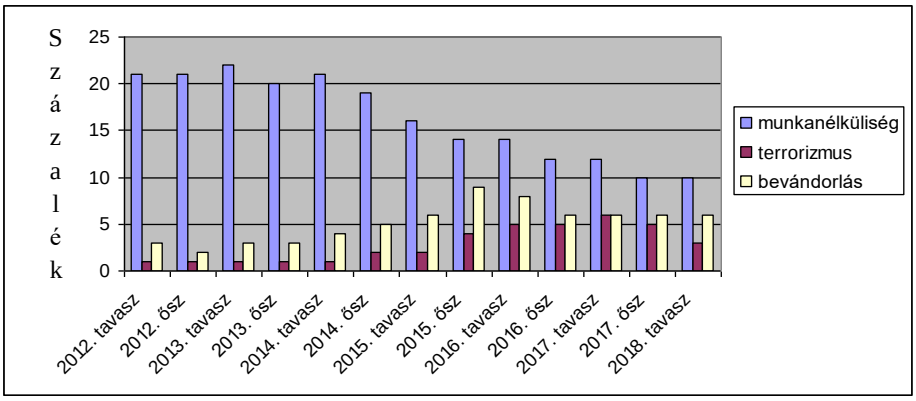


4. ábra: Az interjúalanyok által megnevezett uniós szinten megjelenő legfontosabb problémák

Forrás: Standard Eurobarometer 89, Spring 2018, p. 27.

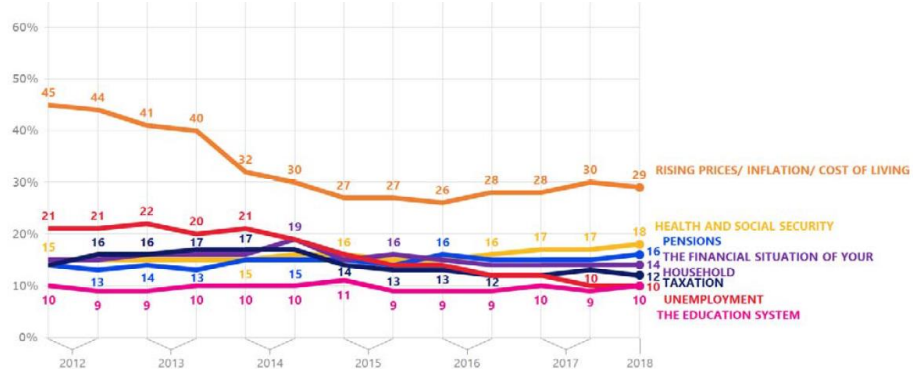
Aminél viszont nem tapasztalható változás, az az egyén szintjén érzékelhető problémák fontossági sorrendje volt, ugyanis a terrorizmus 2012 tavaszától 2018 tavaszáig kivétel nélkül az utolsó helyre került, vagyis az átlagot tekintve az interjúalanyoknak csak 1-6%-a gondolta úgy, hogy neki személy szerint a terrorizmus a fontos kihívások közé tartozik.

[7] 2016. tavasz: 39%; 2016. ősz: 32%; 2017. tavasz: 44%; 2017. ősz: 38%; 2018. tavasz: 29%.



5. ábra: Az egyéni szinten megjelenő problémák közül a terrorizmustól való félelem alakulása összevetve a munkanélküliségtől és a bevándorlástól való félelemmel 2012 tavasza és 2018 tavasza között

Forrás: Standard Eurobarometer 77-89. Készítette a szerző.



6. ábra: A megkérdezettek által említett egyéni szinten jelentkező legfontosabb problémák és kérdések

Forrás: Standard Eurobarometer 89, Spring 2018, p. 12.

A felmérések adataiból azt a következtetést lehet levonni, hogy az Európai Unió lakosai körében 2014 őszéig-2015 tavaszáig a terrorizmus nem került be a legfontosabb kérdések közé sem egyéni, sem országos, sem pedig uniós szinten, mert a fontossági sorrendben mindig valahol középtájon, vagy még hátrébb helyezkedett el. A vizsgált időszakban egészen 2015 őszéig a terrorizmust sokszor olyan kérdések előzték meg, mint a munkanélküliség, a gazdasági helyzet, az infláció és az ehhez kapcsolódó áremelkedés, a bevándorlás, a köztörvényes bűncselekményektől való félelem, valamint az oktatási rendszer állapota, míg a terrorizmus után a listán legtöbbször olyan kérdések következtek, mint például a lakhatás, a nyugdíjrendszer, az államadósság és a klímaváltozás.

A legmagasabb fenyegetettség-percepcióval rendelkező EU-s országok

Az EU-s országok közül 2012 tavasza és 2018 tavasza között az egyéni szintet tekintve legtöbbször Olaszországban és Belgiumban volt a legnagyobb a terrorizmustól való félelem, ami azt jelenti, hogy Olaszországban a válaszadók 2-4%-a, Belgiumban pedig az interjúalanyok 3-11%-a gondolta azt, hogy a terrorizmus az egyén szintjén is megjelenő jelentős kihívások közé tartozik. Rajtuk kívül olyan országok is az átlagnál[8] fontosabbnak tartották a terrorizmust, mint Dánia, Luxemburg, az Egyesült Királyság és Málta, de mindehhez hozzá kell tenni, hogy két kivételtől eltekintve[9] mindegyik országban a megkérdezettek kevesebb mint 10%-a gondolta egyéni szinten lényeges problémának a terrorizmust. Összehasonlításképpen Olaszországban az adózás mellett az áremelkedést tartották a legjelentősebb problémának (41-45%), míg Belgiumban és az Egyesült Királyságban – a legtöbb országhoz hasonlóan – szintén az áremelkedés számított a legkiemelkedőbb problémának.[10]

Országos szinten a terrorizmust legtöbbször Németországban, az Egyesült Királyságban, Belgiumban és Franciaországban ítélték fontos problémának,[11] hozzátéve, hogy 2014 őszéig-2015 tavaszáig mindegyik országban vagy a közepesen fontos, vagy a kevésbé lényeges problémák közé sorolták a válaszadók a terrorizmus jelenségét, vagyis az emberek véleménye ezen a szinten is 2014 végén-2015 elején kezdett megváltozni. Mindamellett általában véve a válaszadók a nemzeti szinten megjelenő kihívások közül Németországban az államadósságot (34-37%) és a bevándorlást (37-56%), az Egyesült Királyságban a munkanélküliséget (35-36%), a bevándorlást (38-44%), valamint az egészségügy helyzetét és a szociális biztonságot (30-34%), Franciaországban a munkanélküliséget (40-65%), Belgiumban pedig a munkanélküliséget (45%) és a bevándorlást (26-29%) tartották a legjelentősebb problémáknak. Hozzá kell tenni, hogy Belgiumban a 2016-os tavaszi felmérés során az interjúalanyok számára a terrorizmus volt a legfontosabb nemzeti szinten megjelenő probléma (33%), míg a bevándorlás csak a második helyen szerepelt.

A terrorizmust uniós szinten 2015 tavaszáig elsősorban Bulgária tartotta a legfontosabb kérdésnek az uniós országok közül (11-18%), hozzátéve, hogy a bolgárok számára az Unió szintjén megjelenő kérdések közül a gazdaság helyzete volt a legfontosabb (27-61%). 2015 tavaszától viszont a visegrádi országokban és a balti államokban olyannyira megnőtt a terrorizmustól való félelem, hogy maguk mögé utasították nemcsak Bulgáriát, hanem a ténylegesen nagyobb terrorfenyegetettséggel rendelkező nyugat-európai országokat is. Mindez azt mutatja, hogy a volt szocialista országok jobban féltek a terrorizmustól, mint a kontinens nyugati részén, így az Európai Unióban a terrorizmust 2015 tavaszától elsősorban a visegrádi és a balti államok tekintették az EU egyik legfontosabb kihívásának (2015 tavasza és 2018 tavasza között a visegrádi és a balti országokban

---

8 Az EU-s átlag 1 és 6% között mozgott.

9 Belgiumban a 2016-os tavaszi felmérésnél a válaszadók 11%-a, míg az Egyesült Királyságban a 2017-es tavaszi felmérésnél a válaszadóknak szintén 11%-a vélte úgy, hogy a terrorizmus egyéni szinten a legfontosabb problémák közé tartozik.

10 Belgium: 34-43%, Egyesült Királyság: 32-36%

11 2012 tavasza és 2018 tavasza között az arány Belgiumban 4-33%, az Egyesült Királyságban 4-33%, Franciaországban 13-36%, míg Németországban 3-28% között mozgott. Az EU-s átlag 2 és 19% között ingadozott.

a válaszadók 20-60%-a tekintette a terrorizmust az EU legnagyobb problémájának).[12] Fontos azonban jelezni, hogy ezekben az országokban 2017 tavaszáig a fontossági sorrendben az első helyen kevés kivételtől eltekintve a bevándorlás szerepelt (40% és 72% között mozgott az arány), tehát a bevándorlástól való félelem még a terrorizmus miatti aggodalomnál is nagyobb volt. A 2017 tavaszán végzett felmérés idején a terrorizmustól való félelem pedig erősebbnek bizonyult a bevándorlástól való félelemnél is.

Annak ellenére, hogy Csehországban, Magyarországon, Lengyelországban, Lettországban és Litvániában sorolták a legnagyobb arányban a terrorizmust a legfontosabb uniós szintű kihívások közé, Romániában, Portugáliában, Máltán, Cipruson, Szlovákiában, Észtországban és Horvátországban is magas volt a terrorizmussal kapcsolatos fenyegetettségérzet. Romániában például a 2015-ös tavaszi, a 2017-es tavaszi és őszi, valamint a 2018-as tavaszi felmérés során az adatfelvételben részt vettek szerint ez volt a legfontosabb uniós szinten megjelenő kérdés (28%, 47%, 41% és 30%), megelőzve még a bevándorlást is (21%, 33%, 36% és 29%). Az uniós szintű kihívásokkal kapcsolatos kiugróan magas romániai fenyegetettség-percepciónak nem ismerjük az okát, ugyanis a délkelet-európai ország nincs a terroristák célkeresztjében és nem tekinthető a bevándorlók célországának sem.

A vizsgált időszakban a terrorizmussal összefüggő fenyegetettség-percepció 2016 tavaszán és 2017 tavaszán volt a legmagasabb az EU-s országokban.[13] 2016 őszén valamelyest mérséklődtek a százalékarányok a fél évvel korábbi felméréshez képest, de 2017 tavaszán szinte az összes EU-s országban ismét jelentősen nőtt azoknak a száma, akik a terrorizmust az EU egészét fenyegető, legnagyobb volumenű kihívásnak tekintették, viszont 2018 tavaszára a korábbi felmérések eredményeihez képest mérséklődött a terrorizmustól való félelem.

Az egyes országokkal kapcsolatos adatokból egy meglehetősen furcsa tendencia rajzolódik ki. Míg egyéni és országos szinten elsősorban a nyugat- és a dél-európai országok érezték az átlagosnál jelentősebb problémának a terrorizmust, addig uniós szinten inkább a közép- és a kelet-európai országok értékelték az egyik legnagyobb fenyegetésként a terrorizmust, vagyis azok az országok, amelyek nem kifejezetten számítanak a bevándorlók célországának, és ahol a terrorfenyegetettség meglehetősen alacsony. Bár tény, hogy az Európai Unión belüli terrorizmussal foglalkozó, évente megjelenő Europol-jelentések (Terrorism Situation and Trend Report – TE-SAT) adatai szerint Romániában és Bulgáriában számos vallási indíttatású terrorizmussal kapcsolatba hozott gyanúsítottat vettek őrizetbe az elmúlt években, de az esetek közül szinte egy sem jutott el az ítélethozatalig. Most nem beszélve arról, hogy 2005 és 2018 között Bulgáriában mindössze egy olyan terrorcselekmény történt, ami vallási indíttatásúnak tekinthető, Romániában pedig

[12] Ez az arány annak fényében számít kiugrónak, hogy az EU-s átlag 2012 tavasza és 2018 tavasza között 5 és 44%, ezen belül 2015 tavasza és 2018 tavasza között 17 és 44% között mozgott.

[13] A 2016-os tavaszi felmérésnél a válaszadók 39%-a, míg a 2017-es tavaszi felmérés során a megkérdezettek 44%-a tekintette a terrorizmust az uniós szinten megjelenő egyik legfontosabb problémának. Emellett az egyén szintjén és az országos szinten jelentkező kihívások megítélésénél is a válaszadók a korábbi felmérésekhez képest fontosabbnak ítélték meg a terrorizmust.

egy sem.[14] A balti és a visegrádi államokat illetően szintén nem beszélhetünk arról, hogy a két országcsoport a vallási indíttatású terrorizmus melegágya lenne, ugyanis az egyébként is ritkán előforduló politikai erőszak sokkal inkább a szélsőjobboldal tevékenységében nyilvánul meg és nem a radikális iszlamizmusban. Ugyancsak érdekes, hogy míg a balti és a visegrádi országokban a válaszadók egyéni és nemzeti szinten nem érzékelik nagyon fontos kérdésnek a terrorizmust, addig uniós szinten (vagyis az EU-ra nézve) a bevándorlás mellett 2015 tavasza és 2018 tavasza között ezt tekintették a legnagyobb kihívásnak.

A terrorizmussal kapcsolatos magas fenyegetettség-percepció általában véve azoknál az országoknál érhető tetten, ahol gyakran követnek el, vagy próbálnak meg elkövetni terrorcselekményt. Ugyanakkor a tapasztalatok azt mutatják, hogy ez az állapot átmeneti, mert amint egy viszonylagos nyugalmi időszak következik, a terrorizmustól való félelem csökken, és a legfontosabb kérdések közé ismét olyan problémák kerülnek be, mint a munkanélküliség vagy az áremelkedés.[15]

A nemzeti szintet illetően, 2014 őszétől kezdve az Egyesült Királyságban, Belgiumban és Franciaországban feltehetően azért volt magas a terrorizmustól való félelem, mert élénken éltek a lakosság emlékezetében a 2014 óta elkövetett merényletek és merényletkísérletek, hozzátéve, hogy bár az Eurobarometer nem tesz különbséget a terrorizmus válfajai között, így nem tudjuk pontosan, hogy a terrorizmustól való félelem a terrorizmus mely típusára vonatkozik, de eléggé valószínű, hogy a vallási indíttatásúra. Viszont annak okát, hogy 2015 tavasza óta a válaszadók szerint a terrorizmus az EU egyik legnagyobb kihívása, nem lehet csak és kizárólag a stratégiai jelentőségű terrorcselekmények és a különböző merényletkísérletek okozta sokkhatásban keresni. Az Iszlám Állam vérengzéseiről szóló hírek is csak részben járulhattak hozzá a fenyegetettségérzet növekedéséhez, ugyanis az al-Kaida különböző helyi szervezeteinek és sejtjeinek véres merényletei már több mint egy évtizede vezető hírei a különböző médiatermékeknek. A félelemérzet növekedése mögött álló legfőbb okot minden bizonnyal a 2015-ös év bevándorlási és menekülthullámával kapcsolatosan kell keresni, ugyanis a válaszadók már egy jó ideje a bevándorlást a fontosabb problémák között tartják számon (különösen EU-s viszonylatban). Mindez oda vezetett, hogy a megkérdezettek a 2015. őszi felmérés során az uniós szinten megjelenő problémák értékelésénél a bevándorlást tették az első helyre, míg a második helyre a terrorizmust sorolták, vagyis a válaszadók nagy valószínűséggel összekapcsolták a 2015-ös év terrortámadásait a bevándorlással és a menekültkérdéssel. Annak ellenére, hogy 2016 őszén mind a terrorizmus, mind a bevándorlás hátrébb szorult a fontossági sorrendben nemcsak a nemzeti, hanem az uniós szintű kihívások megítélésében is, 2017 tavaszára az interjúalanyok szerint már a terrorizmus vált az

---

[14] 2012-ben a bulgáriai Burgaszban egy öngyilkos merénylő terrortámadást hajtott végre izraeli turisták ellen. Annak ellenére, hogy a merényletért a Hezbollahot tették felelőssé, a TE-SAT 2013-as jelentése nem vallási indíttatású terrorcselekménynek tekintette a támadást, mert a kiadvány összeállításának idején még nagyon kevés információ állt rendelkezésre a merénylettel kapcsolatban. Lásd: TE-SAT 2013, https://www.europol.europa.eu/activities-services/main-reports/te-sat-2013-eu-terrorism-situation-and-trend-report, p. 42. (Letöltés ideje: 2018. 11. 10.)

[15] BUREŠ, Oldřich: Perceptions of the Terrorist Threat among EU Member States; In: Central European Journal of International and Security Studies, 2010. 4. évfolyam. 1. sz. p. 66.

EU elsőszámú problémájává. Az ezzel kapcsolatos eredmények mögött minden bizonnyal a 2016-os őszi és a 2017-es tavaszi felmérés közötti fél évben végrehajtott vallási indíttatású merényletek sokkhatását, és az ezzel kapcsolatos médiakampányt kell keresni.[16]

A terrorizmus és a bevándorlás összekapcsolása

Annak ellenére, hogy a vizsgált időszakban a terrorizmustól való félelem hosszú ideig nem volt erős, a közvélekedésben a terrorizmus felől jövő fenyegetés már egy ideje összekapcsolódik a bevándorlókkal, a menekültekkel, de különösen a muszlimok integrációjának, beilleszkedésének kérdésével, valamint a muszlimok feltételezett számarányával. Vagyis minél nagyobb a félelem a terrortól, annál inkább növekszik a muzulmán kisebbségtől való félelem, ráadásul úgy, hogy az európai átlagpolgárnak sem a terrorfenyegetettség mértékéről, sem a muszlimok integrációjának mértékéről, sem a muzulmánok arányáról és problémáiról nincs pontos fogalma.[17]

A muszlimokkal szembeni előítélet és a vallási indíttatású radikalizmussal kapcsolatos félelemérzet a 2015-ös menekültválság időszakában, valamint a párizsi merényletek után vált erősen érzékelhetővé, és a helyzeten egyáltalán nem segített, hogy a politikai kommunikáció gyakran lényegében egyenlőségjelet tett a bevándorlók, a menedékkérők és a potenciális terroristák közé. Ezenfelül csakúgy, mint a 2001. szeptember 11-i amerikai, a 2004-es madridi és a 2005-ös a londoni merényletek után,[18] a 2015-ös párizsi, a 2016-os brüsszeli és a 2017-es spanyolországi támadásokat követően is felerősödtek azok a hangok, melyek az iszlám alapelveit tették felelőssé az erőszakos cselekményekért. Ezzel szemben a 2011-es norvégiai tömeggyilkosság után – amit Anders Breivik saját bevallása szerint a kereszténység védelmében követett el – senki sem firtatta azt, hogy a kereszténységnek volt-e bármi szerepe a terrortámadásban.

---

[16] 2016 decembere és 2017. május vége között muszlim szélsőségesek gázolásos (ramming), illetve gázolással egybekötött késeléses terrortámadásokat hajtottak végre Berlinben, Londonban, Stockholmban és Antwerpenben (ez utóbbi egy sikertelen akció volt). Ráadásul a gázolásos merényleteken kívül történt egy robbantással elkövetett öngyilkos merénylet is 2017. május 22-én Manchesterben. Ezenfelül 2017. február 25-én Heidelbergben történt egy olyan gázolással végződő támadás, amit nem szélsőséges muzulmán követett el, és amit a rendőrség nem tekintett terrorcselekménynek, de a közvélemény vélhetően nem mindig tesz különbséget egy terrortámadás és egy mentális zavarokkal küzdő ámokfutó erőszakos cselekedete között. Lásd: German driver arrested after ramming crowd, police say no signs of terrorism; Reuters, 26 February 2017.

[17] Például amikor felmérések keretében számos ország, köztük több európai uniós tagállam lakosait kérdezték meg, hogy szerintük mekkora az országukban a muszlimok aránya, akkor azt a válaszadók mindenhol, vagyis minden országban felülértékelték. Lásd: Perils of Perception – A Fourteen Country Study, Ipsos MORI, 29 October 2014.; Perils of Perception 2016 – A 40-Country Study, Ipsos MORI, 14 December 2016.; DUFFY, Bobby: The Perils of Perception: Why We're Wrong About Nearly Everything, Ipsos MORI, 8 September 2018.

[18] ROSTOVÁNYI Zsolt: Európai (euro-)iszlám vagy iszlám Európában; In: ROSTOVÁNYI Zsolt (szerk.): Az iszlám Európában; Budapest, 2010, Aula. p. 19.

Konklúzió

Összességében elmondható, hogy a vizsgált időszakban egészen 2014 végéig-2015 elejéig az uniós országok lakosai nem sorolták a terrorizmust a legjelentősebb problémák közé, ugyanis a fontossági sorrendben a terrorizmust mindenhol megelőzték a mindennapi élettel kapcsolatos egyéb problémák, mint például a munkanélküliség és a gazdasági helyzet. 2015-öt követően viszont érezhetően nőtt a terrorizmustól való félelem, ami elsősorban az uniós szintű, kisebb részben pedig a nemzeti szintű problémák értékelésénél jelent meg.

A felmérések eredményeinél feltűnő, hogy mennyire elválik egymástól az, hogy lényegében ugyanazokat a kérdéseket a válaszadók mekkora mértékben tekintik uniós szintű és mekkora mértékben nemzetállami szintű kihívásnak. Emellett azok az országok, amelyeknek alacsony a terrorfenyegetettsége és nincs tapasztalata a bevándorlókkal való együttélést illetően, általában véve uniós szinten nagyobb problémának tekintik a terrorizmust, mint a jóval magasabb terrorfenyegetettséggel rendelkező országok.[19] Ugyanakkor az alacsony terrorfenyegetettséggel rendelkező visegrádi, balti és délkelet-európai országok a nyugat- és a dél-európai országokhoz hasonlóan egyéni és nemzeti szinten már jóval kevésbé tartják fontos kérdésnek a terrorizmust.

Azoknál a nyugat-, közép- és észak-európai országoknál (Franciaország, Belgium, Egyesült Királyság, Németország, Dánia), ahol tartósan magasnak mondható a fenyegetettség-percepció, leginkább a merényletek és a merényletkísérletek sokkhatása köszön vissza. A fenyegetettségérzet növekedésében vélhetően igen fontos szerepük volt részben a 2015 óta megszaporodott vallási indíttatású terrortámadásoknak, az Iszlám Állam brutális gyilkosságairól szóló híradásoknak, a bevándorlási és menekülthullámnak, illetve a politikai kommunikációnak is.

Felhasznált irodalom:

- BUREŠ, Oldřich: Perceptions of the Terrorist Threat among EU Member States, In: Central European Journal of International and Security Studies, 2010. 4. évfolyam. 1. sz. pp. 51–80. ISSN 1802-548X http://www.cejiss.org/static/data/uploaded/13835988933570/3_0.pdf (Letöltés ideje: 2018. 11. 24.).
- DUFFY, Bobby: The Perils of Perception: Why We're Wrong About Nearly Everything, Ipsos MORI, 8 September 2018. https://perils.ipsos.com/slides/index.html (Letöltés ideje: 2018. 11. 29.)

[19] Hozzá kell tenni, hogy a 2017-es tavaszi és őszi, valamint a 2018-as tavaszi felmérésnél a legtöbb kelet- és közép-európai országhoz hasonlóan már számos olyan dél- és nyugat-európai ország is az első helyre tette a terrorizmust, amik korábban nem tekintették ezt a jelenséget az EU első számú problémájának.

- ROSTOVÁNYI Zsolt: Európai (euro-)iszlám vagy iszlám Európában, In: ROSTOVÁNYI Zsolt (szerk.): Az iszlám Európában, Budapest, 2010, Aula. pp. 13-97.
- Eurobarometer – az európai lakmusz, Európa Pont, 2013. 03. 29. http://europapont.blog.hu/2013/03/29/eurobarometer (Letöltés ideje: 2018. 11. 25.)
- German driver arrested after ramming crowd, police say no signs of terrorism, Reuters, 26 February 2017. http://www.reuters.com/article/us-germany-attack-idUSKBN1650OI (Letöltés ideje: 2018. 11. 19.)
- Perils of Perception – A Fourteen Country Study, Ipsos MORI, 29 October 2014. https://www.ipsos.com/ipsos-mori/en-uk/perceptions-are-not-reality-things-world-gets-wrong (Letöltés ideje: 2018. 11. 29.)
- Perils of Perception 2016 – A 40-Country Study, Ipsos MORI, 14 December 2016. https://www.ipsos-mori.com/researchpublications/researcharchive/3817/Perceptions-are-not-reality-what-the-world-gets-wrong.aspx (Letöltés ideje: 2018. 11. 29.)
- Standard Eurobarometer 77, Spring 2012, az Európai Bizottság hivatalos honlapja, 2012. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/63151 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 78, Autumn 2012, az Európai Bizottság hivatalos honlapja, 2013. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/63169 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 79, Spring 2013, az Európai Bizottság hivatalos honlapja, 2013. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/63191 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 80, Autumn 2013, az Európai Bizottság hivatalos honlapja, 2014. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/63206 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 81, Spring 2014, az Európai Bizottság hivatalos honlapja, 2014. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/63226 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 82, Autumn 2014, az Európai Bizottság hivatalos honlapja, 2015. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/71844 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 83, Spring 2015, az Európai Bizottság hivatalos honlapja, 2015. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/68710 (Letöltés ideje: 2018. 11. 09.)

- Standard Eurobarometer 84, Autumn 2015, az Európai Bizottság hivatalos honlapja, 2016. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/72826 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 85, Spring 2016, az Európai Bizottság hivatalos honlapja, 2016. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/77320 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 86, Autumn 2016, az Európai Bizottság hivatalos honlapja, 2017. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79408 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 87, Spring 2017, az Európai Bizottság hivatalos honlapja, 2017. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82870 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 88, Autumn 2017, az Európai Bizottság hivatalos honlapja, 2018. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82873 (Letöltés ideje: 2018. 11. 09.)
- Standard Eurobarometer 89, Spring 2018, az Európai Bizottság hivatalos honlapja, 2018. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/83546 (Letöltés ideje: 2018. 11. 09.)
- TE-SAT 2013, Europol, 2013. https://www.europol.europa.eu/activities-services/main-reports/te-sat-2013-eu-terrorism-situation-and-trend-report (Letöltés ideje: 2018. 11. 10.)

KOÓS GÁBOR – PROF. DR. SZTERNÁK GYÖRGY

A SZÍRIAI POLGÁRHÁBORÚ GEOPOLITIKAI, GEOSTRATÉGIAI HÁTTERE, AZ OROSZ KATONAI MŰVELETEK JELLEMZŐI

Bevezető

Tanulmányunk megírásakor még nem lehetett tudni a szíriai polgárháború befejezésének eseményeit, időpontját, csupán az volt ismert, hogy a békéhez, a befejezéshez vezető út nem lesz egyszerű.

Hét év telt el azóta, hogy kitört a szíriai konfliktus, halált és elnéptelenedett városokat hagyva maga után. Becslések szerint félmilliónál is több szíriait öltek meg a harcokban, és 6,1 millióan távoztak külföldre. Éveken át tartó, városokat kiéheztető ostromok, történelmileg felbecsülhetetlen értékű tájak és emlékművek tönkretétele közben az ország infrastruktúrájának nagy része a földdel lett egyenlővé.

A hét éve tartó szíriai polgárháborúban az Oroszországi Föderáció a Bassár el-Aszad elnök legfőbb támogatója, a szíriai kormányerők gyakorlatilag az orosz fegyveres erők hatékony katonai műveletei révén tudták megfordítani saját javukra a katonai konfliktus menetét. Az északnyugati Idlib tartomány az utolsó olyan nagyobb szíriai régió, amely még a felkelők ellenőrzése alatt áll. Idlib északi részén 2017-ben kialakítottak egy övezetet, ahová olyan lázadók költöztek családjukkal, akik a szíriai kormánnyal kötött egyezségek keretében a polgárháború dúlta ország más részeiből elvonulhattak.

A 2018. szeptember 17-én született orosz-török megállapodás egy 15-20 kilométeres demilitarizált övezetet jelölt ki, ahonnan október 15-ig a lázadóknak ki kellett volna vonulniuk. A megállapodás előírta továbbá a nehézfegyverek eltávolítását is.

2018. október 20-án közzétett nyilatkozatában az Idlib nagy részét ellenőrző dzsihadista ernyőszervezet, a Hajját Tahrír as-Sám, amely az al-Kaida terrorszervezet korábbi szíriai szárnyából, az an-Nuszra Frontból létrehozott Dzsabhat Fatah as-Sám vezetése alatt áll, azt mondta, folytatni akarja a harcot és nem adja át a fegyvereit. Pontosabban: *„Nem adjuk fel az általunk választott dzsihádot és a harcot áldásos forradalmunk céljainak megvalósítására. Nem adjuk át a fegyvereinket.”* A szíriai polgárháború katonai műveleteiről bővebben olvashatunk az Egyesült Államok Vezérkari Főnökök Egyesített Bizottságának elnökével, General Joseph Dunford tábornokkal, és az Oroszországi Föderáció Fegyveres Erőinek vezérkari főnökével, Valerij Geraszimov tábornokkal készült interjúban.[1]

[1] Top U.S. general warns against major assault on Syria's Idlib. https://www.reuters.com/article/us-mideast-crisis-syria-dunford/top-u-s-general-warns-against-major-assault-on-syrias-idlib-idUSKCN1LK1JP (Letöltés ideje: 2018. 10. 15.)

Geopolitikai háttér

1916 májusában Nagy-Britannia és Franciaország képviselői titkos egyezmény írtak alá a Közel-Kelet felosztásáról, miután legyőzték az Oszmán Birodalmat. Az egyezmény aláírását hónapokon át tartó tárgyalások előzték meg, amelyeket a francia jogász, Francois Georges Picot és az angol Mark Sykes vezettek. Tulajdonképpen az ő nevük után kapta az egyezmény a ma is ismert nevét. A közel-keleti államok történészei, szakemberei szerint az egyezmény a nagyhatalmi intrika, az árulás és az akkori arab világ európai lenézésének példája. A térségben élő arabok, kurdok, maronita keresztények a Sykes-Picot-egyezmény alapján ismerték meg, hogy a nagyhatalmi (nyugati) ígéretek mögött nincs semmi. Az ígéreteket mindig felülírják a nagyhatalmi érdekek.

A Sykes-Picot-egyezmény értelmében Szíria kezdettől fogva mesterséges ország, amit az első világháború után hoztak létre az Oszmán Birodalomhoz tartozó történelmi Szíria régió és Észak-Mezopotámia egy részéből. Határai mesterséges határok, amelyek közé rengeteg nép és vallás szorult. A függetlenség 1946-os elnyerésétől kezdve a polgárháború kitöréséig, 2011 márciusáig, az ország kormánya megpróbált ebből az alaphelyzetből kiindulva létrehozni egy szekuláris arab nemzetállamot. A terv azonban megbukott, és abban a formában már nem is indítható újra.

A háború befejezése után várható Szíria felosztása, legalább három részre: az Aszad-féle államra, a kurdok területére, illetve az Erdogan-féle északi bábállamra. Idlib sorsa ebben a változatban teljesen nyitott. Szíria klasszikus „befagyott" konfliktussá alakulna, mint Észak-Ciprus.

Ami a háborút illeti, az még folytatódik: a szír hadsereg most a déli, jordán-izraeli határvidéken készülődik offenzívára, azon a területen, amit a szabad szír felkelők maradéka tart az ellenőrzése alatt a polgárháború kezdete óta.

Janine di Giovanni könyvének[2] ismertetőjében a szíriai polgárháborúról a következők olvashatók: „*2011 márciusában kezdődött eleinte kormányellenes demonstrációkkal, a tunéziai események hatására. Az emberek a jelenlegi politikai elit autoritárius hatalomgyakorlása ellen tiltakozva vonultak utcára, de a*

Интервью начальника Генштаба ВС РФ Герасимова об итогах операции ВС РФ в Сирии и о дальнейших перспективах сирийской войны. https://news-front.info/2017/12/27/intervyu-nachalnika-genshtaba-vs-rf-gerasimova-ob-itogah-operatsii-vs-rf-v-sirii-i-o-dalnejshih-perspektivah-sirijskoj-vojny/ (Letöltés ideje: 2018. 10. 15.)

[2] Janine di Giovanni több mint két évtizeden át dolgozott a Közel-Keleten. A szíriai forradalmat kitörése óta figyelemmel kíséri, 2012 és 2016 között többször is járt az országban. Könyvében elmeséli azoknak az ellenzéki aktivistáknak a történetét, akiket a legkisebb provokációért börtönbe vetettek, és beszámol a damaszkuszi elit szállodákban rendezett fényes fogadásairól, míg a közelben bombák hullnak. A reggel, amikor eljöttek értünk hiteles tudósítás arról, hogyan kerül az összeomlás szélére egy önmagát toleránsnak tartó multikulturális társadalom, és hogyan fordul szomszéd a szomszéd ellen. Szenvedéllyel, félelem nélkül és érzékletesen megírt mű egy széteső ország hétköznapjairól és a legborzalmasabb körülmények között is megmutatkozó emberi ellenállásról. Janine DI GIOVANNI: A reggel, amikor eljöttek értünk. HVG Kiadó Budapest 2017, p. 215. ISBN: 9789633045091

demonstrálók kezdetben csak reformokat követeltek, nem rezsimváltást. A rendfenntartók erőszakos beavatkozása miatt a tüntetések zavargássá fajultak, majd a rendőrség éles lőszerrel lőtt az emberekre, a lázongások gyorsabb elfojtása érdekében pedig harckocsikat is bevetettek.

Novembertől a Rijád el-Aszad tábornok vezetésével megalakult Szabad Szíriai Hadsereg indított gerillaháborút a kormány hadsereg ellen. A kezdetben kizárólag könnyűfegyverekkel rendelkező lázadók a szomszédos arab országok és Törökország hathatós támogatásával jelentős katonai erővé nőtték ki magukat, 2012 őszéig már az ország több települését ellenőrzésük alá vonták. A helyzetet azonban tovább bonyolította, hogy 2012 nyarán az ország északkeleti részén lakó kurdok milíciái is beavatkoztak a harcba, Aleppóig nyomulva előre. A kurd lázadók egyszerre kerültek összetűzésbe a kormányerőkkel és a Szabad Szíriai Hadsereggel. Mindemellett a konfliktusnak erősen szektariánus jelleget ad az a tény is, hogy a helybéli keresztények és alaviták a többségben alavitákból álló Aszad-rezsimet támogatják, míg a lázadók többsége a szunnita lakosság soraiból kerül ki. A szélsőségesebb felkelők rendszeresen hajtanak végre támadásokat a keresztény és alavita közösség ellen, míg a hadsereg és a kormányt támogató Sabiha milícia az ellenzéket támogató szíriai települések lakossága közt rendez időnként kisebb-nagyobb vérfürdőket.

2012. júniusának közepére az ellenzék és a kormányerők közötti harc annyira kiszélesedett, hogy az ENSZ vezető személyei és az Egyesült Államok a felkelést már szabályos polgárháborúnak minősítették."

A konfliktus mögött húzódó okok elsősorban a szíriai társadalom nemzetiségi és vallási megosztottságára vezethetőek vissza. A lakosság mintegy 10-15%-át kitevő kurdok elnyomása az élet több területén is érezhető, de még ennél is fontosabb az a feszültség, amely az ország 75%-át kitevő szunnita lakosság és a mindössze 6 százaléknyi alavita kisebbség között tapasztalható.

A szunniták évekig háttérbe szorítva érezték magukat a kis arányuk ellenére az elitet alkotó alavitákkal szemben, hiszen Bassár el-Aszad elnök és az ő hívei is az iszlám síita ágát képviselő alavita felekezethez tartoznak. Ennek a kis csoportnak a kezében van Szíriában az országot ténylegesen uraló hadsereg és államrendőrség, valamint a forradalom előtt az állami vezető posztok legtöbbjét is birtokolták.

A rendet Szíriában Bassár el-Aszad elnöksége alatt kegyetlen rendőrállam tartotta fent, biztosítva az alavita elit kiváltságait. Mindez keserűséget szült, és a szunniták az arab forradalmak lendületét kihasználva elérkezettnek látták az időt, hogy elűzzék az őket háttérbe szorító kormányt, és ehhez a harcukhoz széles tömegek támogatását is képesek voltak elnyerni, hiszen a szíriaiak egy része is elégedetlen volt az országban zajló folyamatokkal.

Megjegyezzük, hogy a lázadó csoportok nemcsak a kormány, hanem egymás ellen is harcolnak. A Szabad Szíriai Hadsereg olyan kisebb milíciákkal küzd, amelyek helyi vezetőkhöz hűek.

A problémát tovább bonyolítja, hogy a szíriai fiataloknál is betelt a pohár a munkanélküliséggel és az alacsony bérekkel, a korrupcióval és a szigorú

diktatúrával, azzal, hogy csak egy pártra lehetett szavazni, és üldözik az eltérő politikai véleményt képviselőket.[3]

A konfliktus a történelmi helyszíneket sem kímélte: az UNESCO az ország hat világörökségi helyszínének mindegyikét veszélyeztetetté nyilvánította. A világszervezet elsősorban a heves harcok sújtotta Aleppo óvárosának állapotáért aggódik, a műemlékek nagy részének pusztulását hangoztatja.

A többségében szunnita felkelőket hivatalosan Szaúd-Arábia, Katar, az Öbölmenti államok, Törökország, az Egyesült Államok, az Egyesült Királyság és Franciaország támogatják. Nem állami szinten iraki szunniták, csecsenek, afgánok, nyugat-európai dzsihádisták harcolnak az oldalukon. E széles koalíciót főként Bassár el-Aszad elnök megbuktatásának terve kapcsolja össze, de a vélemények eltérőek a későbbi rendezéssel kapcsolatban, nem utolsó sorban az Iszlám Állam miatt.

A kormányerők támogatása ennél jóval korlátozottabb, 2015 előtt elsősorban Irán és a libanoni Hezbollah nyújtott segítséget, ugyanakkor az Irak lakosságának közel 70%-át kitevő síiták szimpátiájára is számíthatnak. A 2015-ben kezdődő orosz beavatkozás ugyanakkor nagy segítség a területei jelentős részét elveszítő Aszad-kormánynak.

A NATO-tagállamok, az Oroszországi Föderáció és a világ más államai korábban és napjainkban is igen költséges háborút vívnak a Közel-Keleten, a Sykes-Picot-egyezmény alapján kialakított határok, államok védelméért. Megakadályozzák ezzel, hogy az ott élő népek maguk döntsenek a sorsukról. Nagy a valószínűsége annak, hogy az Iszlám Állam[4] legyőzése után felül kell vizsgálni a Sykes-Picot-egyezményt, a létrehozott államok és az ott élő népek bevonásával.[5]

Loretta Napoleoni – aki a terrorizmus nemzetközileg elismert szakértője – „Az iszlamista főnixben" című könyvének ismertetőjében a következőket olvashatjuk: Az Iszlám Állam Abu Muszab al-Zarkavi terrorista vezér dzsihadista vágyálmaként fogant a kilencvenes években. A szervezet napjainkra hatalmas terrorgépezetté nőtt: a saría-törvénykezést önkényes kegyetlenkedésre használja, átrajzolja a Közel-Kelet határait, és nagyobb területet ural, mint Nagy-Britannia. Loretta Napoleoni a hírek mögé nézve bizonyítja, hogy az Iszlám Állam több mint a nyugati média ábrázolta szerencsés bűnözői szervezet: valójában a nemzetépítés új modelljét nyújtja; nem terroristacsoport, hanem veszélyes ellenfél, ami tisztában van a kor igényeivel egy zűrzavaros világban. Napoleoni kötete egyrészt vészjósló, másrészt felettébb zavarba ejtő olvasmány. Zavarba ejtő, mert az itt leírt Iszlám Állam köszönő viszonyban sincs azzal a sematikus képpel, amit a média sugároz – és amelyet nem mellesleg saját maga is erősít a „félelem propagandájával". A szerző értő módon bevezeti az olvasókat a Közel-Kelet közelmúltjába, a különböző vallási frakciók

---

[3] Uo.

[4] Az Iszlám Állam, arabul: الدولة الإسلامية ad-Dawlah al-ʾIslāmiyyah, más néven Iraki és Levantei Iszlám Állam, vagy Iraki és Szíriai Iszlám Állam. Angol rövidítéssel *ISIL* vagy *ISIS* egy szunnita dzsihadista szervezet, mely a világ egyik legismertebb terrorszervezete

[5] SARKADI Zsolt: 100 éve született a titkos megállapodás, ami a mai napig gúzsba köti a Közel-Keletet. https://444.hu/2016/05/16/100-eve-szuletett-a-titkos-megallapodas-ami-a-mai-napig-guzsba-koti-a-kozel-keletet (Letöltés ideje: 2018. 10. 15.)

harcába, és hogy ez hogyan hatott, hogyan alakította át a különféle terrorszervezetek működését. Loretta Napoleoni azon túl, hogy leírja a szervezet születését és működését, legfontosabbnak azt tartja, hogy megértesse velünk, miért vonzó alternatíva egy látszólag barbár, brutális rezsim mind a régió lakossága, mind a nyugati másodgenerációs muszlim fiatalok számára.[6]

A tanulmány további részében azt vizsgáljuk meg, hogy a szíriai polgárháború hogyan vált a közel-keleti térség háborújává? A vizsgálathoz felhasználtuk a Deutsche Welle 2018. április 12-i számában Matthias von Hein, Martin Muno, Jens Thurau, Rahel Klein, Mikhail Bushuev kutatócsoport megjelent elemzését.[7]

A szerzők véleménye szerint a polgárháború kimenetelét nem csupán az Bassár el-Aszad elnökhöz hű erők és az ellenzéki csoportok határozzák meg elsősorban. Számos ország vesz részt közvetve vagy közvetlenül a katonai műveletekben, melyeknek nagyon különbözőek az érdekeik.

Először, az Egyesült Államok az iraki és a líbiai beavatkozások (katonai műveletek) okán kezdetben „óvatosan" viszonyult a szíriai polgárháborúhoz. Az Iszlám Állam által végrehajtott műveletek és annak következményei, a terrorizmus elleni harc azonban határozottabb célokat fogalmazott meg. Az Iszlám Állam megsemmisítése és Irán befolyásának gyengítése a Közel-Keleten.

Másodszor, az Oroszországi Föderáció anyagi és katonai segítsége Bassár el-Aszad elnöknek. Az orosz kormány álláspontja: az Iszlám Állam elleni műveletek végrehajtása, de a gyakorlatban minden ellenzéki erő ellen katonai műveletet folytat a térségben. Az Oroszországi Föderáció célja a katonai segítségnyújtással a következő: a) kilépett a nemzetközi elszigeteltségből; b) jelentős segítséget nyújtani Bassár el-Aszad elnöknek; c) a szíriai Tartúszban található orosz katonai bázis megtartása, mert ez geopolitikai fontosságú az ország számára.[8]

Harmadszor, Szaúd-Arábia – a korábban említett kutatócsoport véleménye szerint – a Bassár el-Aszad elnökkel szembenálló erőket támogatja. Ezzel tulajdonképpen Irán és Szíria kapcsolatát kívánja gyengíteni. Ezért Szaúd-Arábia fegyverekkel támogatja az Iszlám Államot.

Negyedszer, Törökország nem titkolt szándéka: Bassár el-Aszad elnök vezette hatalom megbuktatása. Ezzel a szándékkal együtt a kurdokat is szeretné megsemmisíteni, mert egy kurd autonómia a térségben a törökországi kurdokat is segítené önállósági törekvéseik elérésében. A tanulmány szerzői nem zárják ki a törökországi érdekek hátterében fellelhető történelmi tényeket sem, hiszen a térség az Oszmán Birodalomhoz tartozott korábban.

---

6 Loretta NAPOLEONI: Az iszlamista főnix. Az Iszlám Állam és a Közel-Kelet újrarendeződése. HVG Kiadó Budapest 2015, p. 216. ISBN: 9789633042649

7 Internationale Akteure in Syrien: Wer will was im Bürgerkriegsland? https://www.dw.com/de/internationale-akteure-in-syrien-wer-will-was-im-bürgerkriegsland/a-42678444 (Letöltés ideje: 2018. 10. 15.)

8 Az Oroszországi Föderáció szerepéről bővebben olvashatunk Selján Péter tanulmányában. SELJÁN Péter: Oroszország és a szíriai polgárháború. Nemzet és Biztonság 2016. 5. szám pp. 14-30.

Ötödször, a vallási vezetésű Irán támogatja a Bassár el-Aszad elnökhöz hű erőket, elsősorban fegyverekkel, pénzzel, titkosszolgálati információkkal, de nem utolsó sorban katonai erővel. Irán ezzel a támogatással úgy tünteti fel magát, mint a síita vallás védelmezője. Szíria támogatásának Irán részéről más oka is van: az Egyesült Államok befolyásának gyengítése a térségben. Továbbá, Izrael visszaszorítása és Irak katonai erejének gyengítése, a Perzsa-Öböl Menti Együttműködési Tanács befolyásának visszaszorítása.

Hatodszor, Izrael határainak védelme érdekében értékeli a szíriai polgárháború eseményeit. Ugyanakkor a Golán-fennsík védelme az ország elsődleges célja a Hezbollah erőivel szemben. Továbbá Irán szerepvállalása is zavarja az izraeli vezetést.

A tanulmány első részében már említettük, hogy a háború befejezése után várható Szíria felosztása: legalább három részre.

Más elemzés szerint Donald Trump elnöki adminisztrációja a térség hosszú távú stabilitásának biztosítását az Izraelt körülvevő arab államok minél több, kisebb területre való felosztásában látja. Ez a felosztás egyáltalán nem új keletű, az első ilyen tervről Oded Yinon írt 1982-ben „Izrael stratégiája a nyolcvanas évekre" című cikkében, de hasonló tanulmányt tett közzé a Brookings Institute elemzője, Michael O'Hanlon is.[9]

A tanulmány további részében bővebben elemezzük az Oroszországi Föderáció szerepét a közel-keleti térségben a katonai műveletek jellemzőinek tükrében. Az elemzéshez elsősorban a Valerij Geraszimov az Oroszországi Föderáció Fegyveres Erői vezérkar főnökével készült interjú legfontosabb megállapításait és a megjelent orosz tanulmányokat vettük figyelembe.[10]

Az orosz katonai műveletek jellemzői

A katonai műveletek jellemzői vizsgálata előtt röviden ismertetjük Nyikoláj Kozsanov hosszabb tanulmányának lényegét, amelyet *Völgyes Gyöngyvér fordításában olvashatunk el magyar nyelven.*[11]

---

[9] Mike WHITNEY: Ending Syria's Nightmare will Take Pressure From Below. https://www.counterpunch.org/2017/03/28/ending-syrias-nightmare-will-take-pressure-from-below/ (Letöltés ideje: 2018. 10. 15.)
A Trump Strategy to End Syria's Nightmare. Trump wants to collaborate with Russia—which only works if Syria is broken up into autonomous zones. https://www.wsj.com/articles/a-trump-strategy-to-end-syrias-nightmare-1481847575 (Letöltés ideje: 2018. 10. 15.)

[10] Интервью начальника Генштаба ВС РФ Герасимова об итогах операции ВС РФ в Сирии и о дальнейших перспективах сирийской войны. https://news-front.info/2017/12/27/intervyu-nachalnika-genshtaba-vs-rf-gerasimova-ob-itogah-operatsii-vs-rf-v-sirii-i-o-dalnejshih-perspektivah-sirijskoj-vojny/ (Letöltés ideje: 2018. 10. 15.)

[11] Nikolaï KOŽHANOV: Que cherchent les Russes en Syrie? (Nyikolaj Kozsanov: Mit keresnek az oroszok Szíriában?) https://www.cairn.info/magazine-maniere-de-voir-2018-6-p-68.htm (Letöltés ideje: 2018. 10. 15.)

Az Oroszországi Föderáció 2015-ös szíriai katonai beavatkozása a polgárháború kezdetén nem volt magától értetődő. A háború első évében az orosz kormány úgy vélte, Bassár el-Aszad rendszere képes lesz felülkerekedni, amennyiben védelmet kap a külső beavatkozások ellen. Ez az illúzió fokozatosan szertefoszlott, ahogy egyre súlyosbodtak az összecsapások. Az Oroszországi Föderáció ekkor kísérletet tett Szíria és *„a nemzetközi közösség*" közötti kompromisszumos megállapodásra az ENSZ Közgyűlésben, és az orosz kormány kezdett különbséget tenni Bassár el-Aszad és a szíriai állam között.

2015 szeptemberében a szíriai ellenzék egyre nagyobb területeket foglalt el, és radikalizálódott is, ezért az orosz kormány aggódni kezdett Bassár el-Aszad elnök hatalmának jövőjét illetően, a rendszer közeli összeomlásától tartott. Az orosz biztonságpolitikai és katonai szakértők úgy vélték, hogy katonai és technológiai segítségnyújtással csak meghosszabbíthatják a rendszer agóniáját, de megmenteni azt nem tudják. Az Oroszországi Föderáció nem akarta, hogy Szíria a régió egy újabb dzsihádközpontjává váljon.

Az orosz titkosszolgálat és független elemzők is úgy számoltak, hogy 2015-ben közel 12.000 észak-kaukázusi vagy más orosz régiókból származó, illetve a külföldi csecsen közösségekből érkező oroszajkú harcos volt jelen és küzdött Szíriában különböző iszlamista csoportok soraiban. Így például az an-Nuszra Front és az Ahrar Al-Sham mellett. Ráadásul ezekben a csoportokban már több száz azeri és a volt Szovjetunió közép-ázsiai köztársaságaiból érkező, például tádzsik, illetve üzbég harcos is jelen volt. Ezek nem mind azonosultak az Iszlám Állam ügyével, sem az an-Nuszra Frontéval. Ugyanakkor többen úgy tekintettek a Szíriában folyó harcra, mint a saját országukban majdan megvívandó harcok előkészítő szakaszára.

Oroszországi Föderáció szíriai beavatkozásának egyik legfontosabb célkitűzése a rendszer politikai és katonai erejének helyreállítása volt. Így a bombázások elsődleges csapásai azokat a csoportokat sújtották, amelyek komoly fenyegetést jelentettek Bassár el-Aszad elnök kormányának, beleértve azokat is, amelyek nem voltak iszlamisták, illetve amelyeket a Nyugat nem tekintett terroristáknak. De ezt az orosz kormány sohasem ismerte el, és ma is azt állítja, hogy csak terroristákat vett célba.

Valeríj Geraszimov vezérkar főnökkel készült interjú összefoglalója a Szíriában végrehajtott katonai műveletek eredményeiről, és a szíriai polgárháború jövőbeli befejezésének lehetőségeiről.
„A műveletet alaposan megterveztük, figyelembe vettük az összes kérdést, meghatároztuk a szükséges erőket és eszközöket, figyelembe véve a katonai és a támogató, biztosító összetevőket. Olyan tapasztalattal, hogy gyakorlatilag nem rendelkeztünk nagy katonai kontingensek, csapatok és erők átdobásáról nem szomszédos ország területére. Egy példa volt, csak amikor 1962-ben végrehajtottuk az „ANADIR" hadműveletet, amikor is a Szovjetunió Kubába küldött csapatokat. Az ott szerzett tapasztalatokat is figyelembe vettük. Előnyt jelentett az alegységeinknek, hogy azok hirtelen riasztása – készültségük, valamint készenlétük ellenőrzése korábban megtörtént. Ellenőrzések folyamán begyakorolták a nagytávolságú

---

https://www.magyardiplo.hu/2553-mit-keresnek-az-oroszok-sziriaban (Letöltés ideje: 2018. 10. 15.)

átdobást, átcsoportosítást a szállítás összes formájában légi, vasúti és tengeri úton egyaránt.
Az átcsoportosítás a legnagyobb titokban, rejtve, különleges figyelemkeltés nélkül történt. A khmeimimi légibázisra 50 repülőeszköz került összpontosításra. Az átcsoportosítás közel egy hónap alatt megtörtént, több időre volt szükség a biztosító elemek létrehozására.
A tervezés időszakában is szárazföldi csapatcsoportosítás nélkül számoltunk, mivel a szíriai szárazföldi erők helyzetét értékelve arra a következtetésre jutottunk, hogy hosszú időn keresztül részt vettek a harctevékenységekben, és veszteségeket szenvedtek, a több erőt képviselő egység még képes volt a harcfeladat végrehajtására.
Elsősorban szükség volt a célok felderítésének, kiválogatásának és az objektumok, célok tűzzel való pusztításának, valamint az ellenség vezetési rendszerének megbontására vonatkozó feladatok kérdéseinek megoldására. Ezeket a feladatokat a mi Légi és Kozmikus Erőink, csoportosításaink megoldották. A közvetlen szárazföldi feladatokat, műveleteket a szír alegységek a katonai tanácsadóink segítségével hajtották végre. Ezekben részt vettek a szír hazafias érzelmű néprétegek is, ezért a kezdetektől szárazföldi csapataink alkalmazásával nem számoltunk.
A másik nagy feladatkör a vezetés teljes mélységben történő megszervezésére irányult a harctevékenységben résztvevő csapatok és erők irányába. Ezért a khmeimimi légi bázisra telepítettük a csoportosításunk harcálláspontját és vezetési pontokat telepítettünk a harctevékenységet folytató csapatok irányába.
A terrorista erők ellen folytatott műveletekben már tapasztalattal rendelkezünk, és azt természetesen felhasználtuk/figyelembe vettük. A vezérkar a kezdetektől követte a Szíriában folyó háború eseményeit és megismerte a terrorista csoportok harci sajátosságait. Mi megértettük, hogy az erőszakos cselekedeteken kívül harcászati megoldásokat is alkalmaznak, a terrorista csoportok parancsnokait ezekre a különleges feladatokra a nyugati országok és a közel-keleti államok instruktorai készítették fel. Ott voltak az iraki hadsereg tisztjei is, amíg a harctevékenységek folytak. 1500 harckocsi és páncélozott jármű, valamint még mintegy 1200 ágyú és aknavető volt fegyverzetükben. Ez a mennyiség ténylegesen egy reguláris hadsereg fegyverzete. A terrorista erők létszáma 2015. szeptember 30-án 59 ezer fő volt és az elmúlt két évben, akik a harctevékenységek során nagymennyiségű iraki és szír haditechnikát és fegyvereket zsákmányoltak, és még 10 ezer főt toboroztak.
Két év alatt közülük – az adatink szerint – 60 ezer fő terroristaharcos megsemmisítése megtörtént, ehhez még 2800 fő az Oroszországi Föderáció területéről származott.
2015. szeptember 30-ig az amerikai szövetséges csapatok 7000 légicsapást mértek a terrorista erőkre, melyek ennek ellenére – az Oroszországi Föderáció erőinek hadba lépéséig – az általuk ellenőrzött területet Szíriában 20%-ról 70%-ra növelték. Akkor mivel is foglalkozott az amerikai koalíció? Szerintünk, az amerikai koalíció sem akkor, sem most nem szabott feladatot az Iszlám Állam teljes felszámolására/szétverésére. A nemzetközi koalíció mind ez ideig 8-10 légicsapást mért naponta. A légierőnk kevés repülőerővel 60-70 légicsapást mért naponta az Iszlám Állam infrastruktúráira és objektumaira/bázisaira. A legfeszültebb időszakban naponta 120-140 légicsapást mértünk. Csak ilyen módon lehetett a nemzetközi terrorizmus gerincét megtörni Szíria területén. A napi 8-10 légicsapással láthatóan a nemzetközi koalíciónak más céljai voltak. Az ő céljaik az Asszad erőivel folyatott harcra irányultak, nem pedig az Iszlám Állam megsemmisítésére.

Hogy funkcionált a Nemzeti Védelmi Vezetési Központ, amely ezt a struktúrát működtette?

A Nemzeti Védelmi Vezetési Központ létrehozása kardinálisan változtatta meg az állam katonai szervezetek vezetésével kapcsolatos szemléletét. Részben, ezt mi a szíriai műveletek vezetése kapcsán megtapasztaltuk, amikor is minden híradókapcsolat a rendelkezésre állt, megszervezésre került az adatok napi gyűjtése és a helyzet értékelése is. Kényelmes körülmények között dolgoztunk, és nem szenvedtünk információhiányban sem.

Természetesen sok feladatot oldottunk meg online üzemmódban, például a légierő kötelékek, rakétacsapatok, nagy hatótávolságú manőverező rakétákkal végrehajtott csapásokat valósidőben láttuk a monitorokon. A pilótanélküli repülőeszköz által közölt képet egyidejűleg látja hadseregparancsnok a khmeimimi harcállásponton és mi Moszkvában, de a vezetést a hadseregparancsnok végzi.

Mi a kezdetektől próbáltunk megegyezni, megállapodni az amerikaiak vezette koalícióval és sikerült is egy dolgot elérnünk. Megállapodást kötöttünk, memorandumot írtunk alá a légierő repülési biztonságának betartása érdekében. Ez a megállapodás a mai napig érvényben van és betartjuk. Mi egyezményt írtunk alá a Déli-zóna létrehozásáról az amerikaiakkal és a jordánokkal egyaránt a háború kiterjedésének megakadályozására, a feszültségek csökkentése érdekében. Ez volt az első ilyen zóna Szíriában. Az összes többi javaslatunk a közös művelettervezés, a felderítés vezetése, a terroristák megsemmisítése területén mind ellenállásba ütközött vagy simán megtagadták. Mi nem láttuk az együttműködésre vonatkozó hajlandóságot, habár ez nagyon hasznos lett volna – a közös tervezés, csapások mérése, műveletek vezetése területén stb.

A szíriai kormánycsapatok harctevékenységének kibontakozásával/ kifejlesztésével az Eufráteszhez közeledve a Szíria keleti részén az amerikaiakkal meghatároztuk a Légi és Kozmikus Erők és a nemzetközi koalíció közötti tevékenységi zónákat és határokat. Az Eufrátesztől nyugatra a Légi és Kozmikus Erők, a folyótól keletre pedig az amerikaiak tevékenykedtek, de nem a folyómeder teljes hosszában, csak a deeszkaláció vonalán. A térképeken rögzítésre került Dajr-ez Zaur – Suvar – Abert lava és az Irakba vezető átjáró által határolt terület, amely mintegy 120-130 km-re Abu Kemaljaitól északra helyezkedik el. Ezen a területen közös tevékenységet terveztünk, ahol akkor aktív harctevékenység folyt. Az Eufrátesztől keletre a közös tevékenység időszakában az Légi és Kozmikus Erők és a nemzetközi koalíció légiereje alkalmazásakor a felek kölcsönös értesítése rendben folyt, probléma nem merült fel.

Az amerikaiaknak at-Tanf-ban, Szíria déli részén van egy légibázisuk. A bázis 55 km-es körzetben helyezkedik el Szíria, Jordánia és Irak hármas határánál. Az űr- és egyéb felderítési adatok szerint itt helyezték el azon harcosok csoportjait, osztagait, akik a további katonai műveletekre felkészültek. Nemcsak kiképzésen vettek részt, nemrég a BBC tv-csatorna közölte, hogyan szervezték meg a harcosok Rakkából történő kimenekítését – mintegy négyszáz főt a kurdok segítségével az amerikaiak oltalmazása alatt menekítettek a Shaddadi-táborba Szíria észak-keleti részébe. Ez a kurdok által ellenőrzött terület, és itt is van egy amerikai bázis. Ezen kívül a Shaddadi-táborba érkezett további 800 fő az Eufrátesz keleti területéről, ahol a kurdok támadtak, tehát ezek a megmenekült emberek. Ők valójában az Iszlám Állam harcosai. De, a „megdolgozásuk után szint váltanak", új nevet vesznek fel, mint pl. „Új szíriai hadsereg" és másokat. A feladatuk a helyzet destabilizációja. Tudjuk, hogy az Shaddadi-táborból 400 fő érkezett al-Tanf térségébe, már az után, hogy az Iszlám Állam fő erői megsemmisültek. Ők kísérletet tettek a helyzet

destabilizációjára, miután az Eufrátesz keleti területeiről támadtak, de a szír kormányerőkkel szemben veszteségeket szenvedtek.
Úgy gondoljuk, hogy most mintegy 750 fő al-Shaddadiban, és további 350 fő az at-Tanf bázison található. al-Tanf körül a szír csapatok körbezárták az 55 km-es zónát. A legfontosabb, hogy néhány hónapja megfigyeltük a harcosok előrevonását, távozását, amíg az ellenőrzés gyenge volt, addig az at-Tanf térségéből 350 harcos jutott ki. Küszöbön állt a szír Karjat város elfoglalása. Mi időben intézkedtünk, nagy veszteséget okozva, és ezek az erők felszámolásra kerültek. Hadifoglyok is voltak a táborokban. Világos, hogy ott kiképzés folyt. Sőt Al-Rukbanban található a legnagyobb szíriai menekült tábor is.
Mint ismert, kettő bázis, a Khmeimim légi és Tartusz haditengerészeti marad a fennhatóságunk alatt, teljes mértékben együttműködünk szíriai kormánycsapatokkal, amelyeknél a tanácsadóink alegységszinten is jelen vannak. Ez idő alatt a szír haderő alegységparancsnoki állománya nagy gyakorlatot szerzett a műveletek végrehajtásában, ma már önállóan képesek a harctevékenység vezetésére/irányítására a saját területeiken/felelősségi körzeteikben. A bázisainkon elhelyezett erőkkel részükre a szükséges támogatást biztosítjuk, ez az erő már elegendő a stabilitás biztosítására, és a Szíria területi egysége megtartására. A szír kormány értékelése szerint a helyzet még nem elegendően szilárd. A teljes biztonság eléréséhez még idő kell. Ezért a katonai bázisainkra szükség van. A másik oldalról nem szabad elfelejteni, hogy az Oroszországi Föderációnak saját érdekei is vannak a Közel-Keleten.
A legnehezebb feladat a kezdeti időszakban a szíriai kormányerőkkel, a különféle, a területen harcoló erőkkel-szabadcsapatokkal, a környéken élő hazafias érzelmű lakosság osztagaival való együttműködés megszervezése volt. Ezeket a fegyveres sejteket, osztagokat a kormányerő támogatásába próbáltuk bevonni. Nem volt egyszerű ezen erőknek a mi Légi és Kozmikus Erőkkel történő együttműködését és mindenoldalú biztosítását megszervezni, ezt a feladatot ma már elsajátítottuk, a kialakított keretek között hatékonyan végezzük. Khmeimimben működő harcálláspontunk a csapatokkal való együttműködést Szíria területén rendben végzi.
A műveletek végrehajtásakor folyamatos korrekcióra van szükség, mert az elgondolások, megközelítések, a formák és tevékenységek módjai is változnak. A terroristák először ritkábban, később tömegesen alkalmazták a „dzsihád-mobilokat". Erre természetesen reagálni kellett a Deir ez-Zor-i harcok időszakában, amikor is kezdetben csak 2-3, később már 7-8 ilyen járművet alkalmaztak a harcok folyamán. Ez lehet egy gépjármű, egy harcjármű, vagy harckocsi, esetleg más páncélos eszköz, amit 300-400 kg robbanóanyaggal feltöltenek, egy öngyilkos merénylő vezeti – célja, hogy nagy sebességgel a legrövidebb útvonalon a kormányerők állásaihoz érjen és ott a felrobbantsa azt. Ilyen esetekben pánik, élőerőben nagy veszteség keletkezik és egy széles átjáró nyitása is megtörténik.
Példának említem, hogy 2016-ban az Aleppo környékén folyó harcokban ezzel a módszerrel 3 „dzsihád-mobillal" sikerült a kitörés a gyűrűből. A kormányerők két ellenőrző-áteresztő pontját felrobbantották, 500-700 m széles átjáró keletkezett, a terrorista erők tevékenysége jól tervezett volt, két oldalról támadták a folyosóban lévő erőket és a bekerítésből kitörtek – azután két hónapi nehéz harcok árán sikerült újra zárni a gyűrűt a kormányerőknek…természetesen ez nem fér a hagyományos harctevékenység keretei közé, a következtetéseket pedig le kellett vonni, rendszabályokat kellett foganatosítani.
Ezek: a folyamatos figyelés megszervezése, meghatározásra kerülnek a veszélyes irányok, lehetséges útvonalak, ahol a terrorista osztagok manőverezhetnek. Ezekre

az irányokra csomópontokban akadályokat és aknákat telepítettek, tűzzel történő biztosítást szerveztek (a rendszeresített és meglévő páncéltörő harcjárművek, harckocsik, majd közelebb a kézi páncéltörő rakéták alkalmazásával) a távoli megközelítési útvonalak figyelembevételével. Az eredmény azonnal jelentkezett: 2-3 „dzsihád-mobil" a manőver megkezdését követően, a többiek a peremvonalhoz való közelítés időszakában megsemmisültek. A csapatok megtanulták az ellenállás megszervezését és végrehajtását is.

A tapasztalat szerint az Iszlám Állam harcosai a helyi lakosság bevonásával és kényszerítésével körkörös védelmet szerveztek. A föld alatt jóformán egy másik várost létesítettek, építettek ki teljes infrastruktúrával.

A föld alatt a járatokban folytatandó harcot a különleges erőknek, rohamosztagoknak meg kellett tanulni.

Az Iszlám Állam haditechnikai eszközei sok ország támogatásával, segélyek formájában, de még a Közel-Keletről is, nem kormányzati szervezetek segítségével jutottak Szíriába. De nemcsak járművek, hanem korszerű fegyver, új lőszerek és modern eszközök – felderítő eszközök, távcsövek, éjjellátó készülékek és híradó rendszerek, bizony nem özönvíz előttiek. Már ismert, hogy az Iszlám Állam sok harcosa menekült Afganisztánba, de főleg Líbiába, és Délnyugat-Ázsiába.

Az orosz haderő állományából 48 ezer katona vett részt a műveletekben. Magasra értékelem a tevékenységüket, minden zászlóaljban, dandárban vagy ezredben és hadosztályban ott vannak a tanácsadóink és a szükséges szolgálati személyek is. Ez az operatív csoport felderítő, tüzér, műszaki, tolmács és más szolgálati személyekből áll. Ők a tervező csoportot alkotják, segítik az alegységek vezetését a feladat végrehajtása során.

A vezérkar célja az volt, hogy minél több parancsnok és tiszt vegyen részt a műveletekben. A katonai körzetek parancsnokai is hosszabb időt töltöttek el a hadműveleti területen, mindenki a Szíriában folyó hadműveletek vezetését gyakorolta.

A parancsnokok a saját törzseik állományával érkeztek a hadműveleti, a felderítő, a híradó, a rakéta-tüzér és a műszaki főnökökkel. Megállapítható hogy a teljes hadseregvezetés, a hadosztálytörzsek 90%-a, és az ezredek, dandárok fele komoly tapasztalatot szerzett a hadjárat eddigi időszakában.

A tapasztalatok feldolgozása és általánosítása folyamatosan történik. A hadjárat első napjától kezdve tudományosan megalapozott munkát végzünk, minden esemény részletesen elemzésre kerül. A tapasztalatok átadása konferenciákon, felkészítések alkalmával az alegységek és a katonák szintjére is eljutott. Jó néhány tansegédletet készítettünk.

Mintegy 200 különféle fegyvert, haditechnikai eszközt próbáltunk ki, amiket nem régen rendszeresítettünk, állítottunk hadrendbe. Annak ellenére, hogy kemény tesztelések során ezeket kipróbáltuk, néhány esetben valamilyen probléma jelentkezett. Katonáink a problémákat azonnal jelezték az alkalmazáskor. Szíriában állandó katonai-műszaki, hadtudományos felügyelet mellett alkalmaztuk a haderőnemek fegyverzetét és technikai eszközeit.

Mérnökök, konstruktőrök, hadtudósok, a fejlesztők mind jelen voltak. Minden új típusú fegyver és eszköz előnyös oldalait kielemezték és a jelentkező hiányosságokat már kijavították. Az, hogy harci körülmények között fegyvereinket kipróbáltuk, ez kitűnő lehetőség volt, és növelte a fegyvereink erejében vetett hitet.

Soha nem alkalmaztunk, használtunk ennyi pilótanélküli repülőeszközt, mint Szíriában. Ezek alapvetően a felderítés és a rádióelektronikai harc eszközei, de megoldanak más feladatot is. 5 év alatt hatalmasat léptünk előre a fejlesztésük

területén. Most pilótanélküli repülőeszköz nélkül nem érdemes harctevékenységet folytatni. Ezt alkalmazza a tüzérség, a felderítők, a légierő is. A pilótanélküli repülőeszközükkel alkotjuk meg a felderítő csapásmérő egységeket és hozzuk létre a „felderítő–tűz kontúrokat, kereteket”.[12]
A különleges erőkről el kell mondani, hogy megállták helyüket, a legjobb oldalukról ismerhettük meg őket. A légierő kötelékek közvetlen célravezetésétől az Iszlám Állam vezéreinek megsemmisítéséig, és néhány más feladat megoldásáig. Elégedettek vagyunk az általuk harceljárás során szerzett nélkülözhetetlen tapasztalatokkal.” – fejezte be Valerij Geraszimov.

Az orosz katonai légierő bevetése gyorsan elért két célkitűzést. Először, megnőtt annak az esélye, hogy a szíriai rendszer (Bassár el-Aszad elnök rendszere) hosszú távon fennmaradjon. Másodszor, lehetetlenné tette, hogy a nyugati országok repüléstilalmi zónát hozzanak létre, illetve esélytelenné tett egy közvetlen és sikeres szárazföldi beavatkozást a szíriai kormányerők ellen.

Ami talán ennél a két célkitűzésnél is fontosabb, a polgárháború befejezése szempontjából, nyilvánvaló, hogy semmilyen Szíriával kapcsolatos döntést nem lehet az Oroszországi Föderáció álláspontja ellenére meghozni a jövőben.

Befejezés

A Szíriában végrehajtott orosz katonai műveletek, a „Nyugat-2017” és a „Kelet-2018” gyakorlatok tapasztalatai alapján megállapíthatjuk, hogy az Oroszországi Föderáció tudatosan készíti fel haderejét egy esetleges fegyveres konfliktus megvívására: haderőreformmal, átfegyverzéssel, kiképzéssel, hadászati-hadműveleti gyakorlatokkal, amelyek eredményeként az orosz fegyveres erő napjainkra elérte hadászati-hadműveleti alkalmazhatóságának képességét, azaz a Nyugatnak reális kihívásként kell számolnia vele a hagyományos, valamint a nem-lineáris hadviselés terén egyaránt.

Az orosz fegyveres erő az egyre erősödő tendenciát mutató hagyományos képességekkel párhuzamosan folyamatosan bővíti hadászati rendeltetésű eszköztárát is. Ezek bemutatásával az orosz kormány elérte, hogy tárgyalásra késztesse az Egyesült Államokat és szövetségeseit.[13]

---

[12] A szíriai katonai műveletekben alkalmazott eljárás az ellenséges célok (objektumok) gyors és hatékony pusztítása érdekében. Az eljárásról bővebben olvashatunk a következő tanulmányokban: Lester W. GRAU – Charles K. BARTLES: The Russian Reconnaissance Fire Complex Comes of Age. Changing Character of War Centre Pembroke College, University of Oxford With Axel
Margaret Ax: son Johnson Foundation, May 2018. https://static1.squarespace.com/static/55faab67e4b0914105347194/t/5b17fd67562fa70b3ae0dd24/1528298869210/The+Russian+Reconnaissance+Fire+Complex+Comes+of+Age.pdf (Letöltés ideje: 2018. 10. 15.)
Диана Михайлова: Разведывательно-огневой контур: изменит ли правила войны эта российская военная тактика? https://diana-mihailova.livejournal.com/2570910.html (Letöltés ideje: 2018. 10. 15.)

[13] Readout of Chairman of the Joint Chiefs of Staff Gen. Dunford's Meeting with Russian Chief of the General Staff Gen. Gerasimov, 2018. 06. 08.

Az orosz haderő szíriai katonai műveletei tapasztalata, haditechnikai fejlesztésének és átfegyverzésének eddigi folyamata azt mutatja, hogy az orosz katonai gondolkodás elfogadja a hadtudományi és haditechnikai kutatások eredményeit, azok gyakorlati megvalósításának lehetőségét, a haderőbe történő beintegrálása pedig hatással van a katonai gondolkodásra.

2018. július 16-án megtartott orosz–amerikai elnöki találkozón Vlagyimir Putyin orosz és Donald Trump amerikai elnökök egyeztettek a szíriai politikai és katonai eseményekről, valamint a lehetséges megoldásról is.

Véleményünk szerint az Egyesült Államoknak és az Oroszországi Föderációnak a szíriai polgárháború rendezésével kapcsolatos nézeteltérései, valamint az eddigi tűzszüneti megállapodások kudarca ellenére a jövőben is arra kell majd törekedniük, hogy valamilyen szinten együtt tudjanak működni a szíriai konfliktus lezárása érdekében.

Az Oroszországi Föderáció leginkább azért ellenzi továbbra is Bassár el-Aszad elnök hatalomból való erőszakos eltávolítását, mert komoly kétségei vannak afelől, hogy biztosítható lenne a békés, rendezett hatalmi átmenet, azaz az iraki vagy a líbiai káosz megismétlődésétől tart. Ennek megfelelően az orosz álláspont szerint a legjobb esetben egy hatalommegosztási megállapodás jöhetne létre Szíria különböző politikai és társadalmi szereplői között, Bassár el-Aszad elnök elnököt is bevonva.[14]

Bízunk abban, hogy a jelenlegi szembenállás bizonyos kérdésekben megmarad a párbeszéd lehetőségének szintjén, a folyamatos tárgyalások elősegítik a szíriai kérdés megoldását is az ott élő népek érdekeinek figyelembevételével.

---

http://www.jcs.mil/Media/News/News-Display/Article/1545036/readout-of-chairman-of-the-joint-chiefs-of-staff-gen-dunfords-meeting-with-russ/ (Letöltés ideje: 2018. 06. 11.)

[14] A szíriai polgárháború befejezésének lehetőségéről, a béke megteremtéséről bővebben olvashatunk a következő tanulmányokban:
Jeffrey A. STACEY: Russia's Pyrrhic Victory in Syria Before and After the Drawdown. https://www.foreignaffairs.com/articles/syria/2016-03-20/russia-s-pyrrhic-victory-syria (Letöltés ideje: 2018. 10. 15.)
WAGNER Péter**:** Brutális végjáték kezdődhetett Szíriában. https://24.hu/kulfold/2018/09/08/sziriai-idlib-tamadas/ (Letöltés ideje: 2018. 10. 15.)

Felhasznált irodalom:

- Интервью начальника Генштаба ВС РФ Герасимова об итогах операции ВС РФ в Сирии и о дальнейших перспективах сирийской войны, https://news-front.info/2017/12/27/intervyu-nachalnika-genshtaba-vs-rf-gerasimova-ob-itogah-operatsii-vs-rf-v-sirii-i-o-dalnejshih-perspektivah-sirijskoj-vojny/ (Letöltés ideje: 2018. 10. 15.)
- Гражданская война в Сирии и история политического урегулирования, https://ria.ru/spravka/20180129/1513416087.html (Letöltés ideje: 2018. 10. 15.)
- Как начиналась война в Сирии.http://www.rosbalt.ru/main/2014/03/12/1243302.html (Letöltés ideje: 2018. 10. 15.)
- Истоки начала войны в Сирии. http://новости-сирии.ru-an.info/новости/истоки-начало-войны-в-сирии-как-западные-лидеры-готовились-к-этой-войне/ (Letöltés ideje: 2018. 10. 15.)
- Война в Сирии и Ираке. https://tjournal.ru/56447-explaining-syria-and-iraq (Letöltés ideje: 2018. 10. 15.)
- Why is there a war in Syria? https://www.bbc.com/news/world-middle-east-35806229 (Letöltés ideje: 2018. 10. 15.)
- Turkey, Iran and Russia discuss Syria at trilateral summit in Tehran. https://www.dailysabah.com/politics/2018/09/07/turkey-iran-and-russia-discuss-syria-at-trilateral-summit-in-tehran (Letöltés ideje: 2018. 10. 15.)
- Syria: Rebels comply and pull heavy weapons out of Idlib. https://www.aljazeera.com/news/2018/10/syria-war-rebels-complete-heavy-arms-pullout-idlib-zone-181010145807507.html (Letöltés ideje: 2018. 10. 15.)
- Unintended consequences. https://www.economist.com/special-report/2016/05/14/unintended-consequences (Letöltés ideje: 2018. 10. 15.)
- Jeffrey A. STACEY: Russia's Pyrrhic Victory in Syria Before and After the Drawdown. https://www.foreignaffairs.com/articles/syria/2016-03-20/russia-s-pyrrhic-victory-syria (Letöltés ideje: 2018. 10. 15.)
- Internationale Akteure in Syrien: Wer will was im Bürgerkriegsland? https://www.dw.com/de/internationale-akteure-in-syrien-wer-will-was-im-bürgerkriegsland/a-42678444 (Letöltés ideje: 2018. 10. 15.)
- Nikolaï KOŽHANOV: Que cherchent les Russes en Syrie? (Nyikolaj Kozsanov: Mit keresnek az oroszok Szíriában?) https://www.cairn.info/magazine-maniere-de-voir-2018-6-p-68.htm (Letöltés ideje: 2018. 10. 15.)
- SARKADI Zsolt: 100 éve született a titkos megállapodás, ami a mai napig gúzsba köti a Közel-Keletet. https://444.hu/2016/05/16/100-eve-szuletett-a-titkos-megallapodas-ami-a-mai-napig-guzsba-koti-a-kozel-keletet (Letöltés ideje: 2018. 10. 15.)

DR. ANDREIDES GÁBOR

A TERRORIZMUS HATÁSA ÉS KEZELÉSE OLASZORSZÁGBAN AZ „ÓLOMÉVEK" ALATT

Bevezetés

A száz esztendeje született Giulio Andreotti megkerülhetetlen szereplője volt a második világháborút követő olasz politikatörténetnek. A római születésű kereszténydemokrata politikus jelentősége megkérdőjelezhetetlen az ország második világháborút követő történelmében. Döntő befolyással bírt nemcsak a hetvenes évek politikájára, de jóformán nem is született nélküle fontos politikai döntés az 1946-ban megszületett úgynevezett „első Olasz Köztársaság" történetében. Kapcsolatai széleskörűek voltak, hatalmas befolyással bírt. Kiterjedt ismeretségére már fiatal egyetemista korában szert tett. Jogi tanulmányai alatt, a katolikus egyetemi szövetségben[1] végzett munkája idején ismerkedett például meg a nála két és fél évvel idősebb Aldo Moro-val, aki meghívta diáktársát a szövetség lapjának, az „Azione Fucina" című újságnak a társigazgatói posztjára. Hamar közeli munkatársak lettek, így nem csoda, hogy mikor Moro-nak a sorkatonai szolgálat miatt távoznia kellett az elnöki székből, Andreotti volt az, aki későbbi politikus- és párttársát váltotta. Andreotti és Moro az olasz politikatörténet két kiemelkedő alakja. Ugyannak a politikai családnak voltak a tagjai, mégis eltérő habitusú és jelentősen különböző politikusok voltak. Pályájuk és sorsuk alakulása mintegy jellemzik azt az időszakot, mikor hatalmas kihívásokkal, megoldandó feladatokkal kellett szembenéznie az olasz politikának. Moro 1978-ban meghalt, megölték. Andreotti harmincöt évvel élte túl párttársát. 2013-ban bekövetkezett halálakor a nekrológok többek között a négy évtizeddel ezelőtti Moro-válság idején folytatott politikájának okait firtatták.[2]

1969. december 12-én bomba robbant a Banca Nazionale dell'Agricoltura milánói épületében. A merénylet, amelynek következtében tizenhatan életüket vesztették, hatalmas riadalmat okozott az olasz belpolitikai életben, különösen a baloldalon. Pietro Nenni, az olasz szocialisták (Partito Socialista Italiano) leköszönő titkára, egy esetleges szélsőjobboldali veszélytől tartva azonnal arra az 1921-es, halálos áldozatokat is követelő anarchista robbantásra gondolt, amelyet szintén Milánóban, a Diana Színházban követtek el, és amely szimbolikusan ugyan, de hozzájárult a fasizmus hatalomra kerüléséhez.[3]

Az 1969-es detonációt megelőzően szintén a lombard fővárosban lépett életbe egy kisebb pokolgép, majd még aznap Rómában robbant három, 16 óra 55 perc és 17 óra 30 perc között a Banca Nazionale del Lavoro (via San Basilio) épületében, valamint a Piazza Venezia impozáns emlékművében, a Haza Oltárán (Altare della

[1] Federazione Universitaria Cattolica Italiana – FUCI

[2] PANKOVITS József: Giulio Andreotti (1919-2013) in: http://www.grotius.hu/doc/pub/APKQRJ/2013-08-05_pankovits_jozsef_andreotti.pdf (Letöltés ideje: 2018. 07. 11.)

[3] Aurelio LEPRE: Storia della prima Repubblica. L'Italia dal 1943 al 2004. il Mulino, 2004. p. 245

Patria).[4] Az egymást követő robbanások tragikus időszak eljövetelét jelezték. Az elkövetkező években az olasz államnak nehéz biztonsági problémákkal kellett szembenéznie. A terror – amely ugyan nem volt teljesen ismeretlen az egyesített ország történetében[5] – az olasz hétköznapok részévé vált.[6]

„Ólomévek" („anni di piombo"), ezzel a sokat eláruló jelzővel illetik gyakorlatilag a hatvanas évek végétől a nyolcvanas évek elejéig tartó bal- és jobboldali terrorista akcióktól zaklatott időszakot a demokratikus Olasz Köztársaság történelmében. Merényletek, emberrablások, gyilkosságok, államcsínykísérlet-próbálkozások követték egymást. Ráadásul a „hosszú" hetvenes évek végén, az 1980-as évek elején kitört második maffia-háború még inkább növelte Róma belbiztonsági problémáit. És ezután következett az 1981-ben kipattant P2-botrány[7] is, amely az ólomévek küzdelmeiben megfáradt olasz társadalmat szintén súlyosan érintette. Az általunk vizsgált időszakkal kapcsolatban érdemes kiemelni, hogy ismert a „feszültség stratégiája" („strategia della tensione") politikai teória, miszerint az itáliai társadalom destabilizálása egy jól átgondolt szisztéma volt arra, hogy segítségével meg lehetett akadályozni a fönnálló politikai struktúra megváltozását, a kommunista párt kormányra kerülését.

1. A terror klasszikus időszaka Olaszországban

A stagnáló politikai-gazdasági viszonyai mellet az olasz társadalom egy egyszer már bevált politizálással kezdett ismerkedni. A meghatározó politikai erők, a jobb (kereszténydemokraták) és a bal (kommunisták) összefogására a második világháborút követően ugyanis már volt példa. Ám ekkor, vagyis a hetvenes évek közepén, a megváltozott nemzetközi és hazai viszonyok közepette a politikai elit egyáltalán nem volt felkészülve a javaslatra.

Három esztendővel a milánói robbantást követően az ország közbiztonsági helyzete egyre rosszabbá vált: Megerősödtek a különböző újfasiszta és szélsőjobboldali parlamenten kívüli politikai mozgalmak, csoportosulások. 1969-ben 145 robbantásos merénylet történt az országban, amelyből 96 bizonyosan a

---

4 http://www.memoria.san.beniculturali.it/web/memoria/approfondimenti/scheda-approfondimenti?p_p_id=56_INSTANCE_J1sq&articleId=13602&p_p_lifecycle=1&p_p_state=normal&groupId=11601&viewMode=normal (Letöltés ideje: 2018. 05. 13.)

5 E tekintetben tradicionálisan két nagy felháborodást kiváltó terrorcselekményt szokás említeni. Az egyik az uralkodó, I. Umberto meggyilkolása 1990. július 29-én, a másik Matteo Matteotti elrablása és meggyilkolása 1924. május 30-án. Cossiga

6 LEPRE i. m. p. 245.

7 Tulajdonképpen nem maga a P2 (Propaganda Due) szabadkőműves páholy kavarta föl az indulatokat, hiszen annak létéről – ahogy a szabadkőművességről általában – tudomással voltak. A súlyos belpolitikai feszültség inkább annak volt köszönhető, hogy az elsősorban és hangsúlyozottan antikommunista funkciójú, pártok és bürokrácia feletti informális összekötő szervezetként működött. Erősen jobboldali páholy tagjai között kereszténydemokrata, republikánus, liberális, szocialista, szociáldemokrata, és szélsőjobboldali politikusok, államtitkárok, tartományi elnökök, magas rangú képviselők, újságírók, bankárok, diplomaták voltak. Sőt sokan nem értették, de a tagok között volt Száll József egykori magas rangú diplomata, Magyarország 1962-1970 közötti római nagykövete, aki 1970-ben disszidált és egy hónapos magyarországi tartózkodást követően tért vissza Olaszországba.

szélsőjobb, az úgynevezett „fekete terrorizmus" („terrorismo nero") számlájára volt írható[8]. 1970. december 7-8-ára virradó éjjelen jobboldali államcsíny-kísérlet zajlott Rómában[9]. Juan Valerio Borghese herceg, a szélsőjobb irányában maximálisan nyitott egykori világháborús tengerész-parancsnok[10] irányítása alatt az összeesküvőknek meg kellett volna szállniuk a stratégiailag fontos csomópontokat, majd elhangzott volna Borghese herceg proklamációja. Nem így történt. Az összeesküvőket a rendőrség idejekorán letartóztatta, Borghese Spanyolországba menekült. Az államcsíny gondolatát számos kisebb-nagyobb szélsőjobboldali csoport támogatta. A deklaráltan újfasiszta parlamenti párt, az olasz szociális mozgalom (Movimento Sociale Italiano –MSI) és vezetőjének Giorgio Almiranténak viszonya azonban nem volt ennyire egyértelmű a Borghese-tervvel kapcsolatban. Andreotti egyenesen úgy gondolta, hogy *„nem lehetetlen, hogy a rendőrséget Almirante értesítette. Az MSI távol tartotta magát ettől a bonyodalomtól, képviselői jól elvoltak a demokratikus rendszerben."*[11] 1970. július 22-én szintén szélsőjobboldali terroristák léptek akcióba és robbantottak pokolgépet a calabriai Gioia Tauro település közelében[12], majd 1972. május 31-én a Gorizia megyei Peteano di Sagrado településen.[13] Mindkét terrorcselekmény halálos áldozatokat és több tucat sebesültet követelt.

A politikai-ideológiai háttér és a terrorista akció végrehajtása tekintetében a hetvenes-nyolcvanas évek olaszországi terrorizmusa alapvetően két jellegzetes különbséget mutat. Az eddig ismertetett újfasiszta-szélsőjobboldali ideológiai csoportok erőszakos akciói a „minél nagyobb, annál jobb" stratégiáját követték, terrorcselekményeik számtalan ártatlan áldozatot követeltek („terrorismo stragista"). A szélsőbaloldali gyökerű csoportosulások ezzel szemben lényegét tekintve egyes személyek, politikusok, ügyészek-vizsgálóbírók, nagyiparosok, újságírók, magas rangú csendőrök és rendőrök ellen intéztek támadásokat („terrorismo brigatista").[14]

Mindennek ismeretében egyáltalán nem meglepő, hogy Giulio Andreotti második kormányának[15] parlamenti bemutatkozásakor, 1972. július 4-én a kormányfő, ha akart sem tudott volna nem foglalkozni az egyre romló közbiztonsági

---

8 http://mappedimemoria.it/stragi/gli-anni-delle-stragi/ (Letöltés ideje: 2018. 05. 15.). Szélsőjobboldali terrorszervezetek voltak többek között: Ordine nuovo, Avanguardia nazionale, Ordine nero

9 LEPRE i. m. p. 245.

10 FRANZINELLI, Mimmo: RSI. La repubblica del duce 1943-1945 Oscar Mondadori, 2011, p. 86.

11 Giulio Andreottit idézi Bruno Vespa. Lásd: VESPA, Bruno: Storia d'Italia da Mussolini a Berlusconi. Mondadori Rai, 2004. p. 170

12 http://www.memoria.san.beniculturali.it/web/memoria/approfondimenti/scheda-approfondimenti?p_p_id=56_INSTANCE_J1sq&articleId=13610&p_p_lifecycle=1&p_p_state=normal&groupId=11601&viewMode=normal (Letöltés ideje: 2018. 05. 24.)

13 https://www.youtube.com/watch?v=ckjJDyh4oVA (Letöltés ideje: 2018. 05. 13.)

14 MARLETTI, Carlo: Uccidere in nome delle idee Continuità e mutamenti del terrorismo ideologico e politico degli anni settanta e ottanta in: http://www.fondazioneveranocentini.it/index.php?option=com_content&view=article&id=139:uccidere-in-nome-delle-idee&catid=67&Itemid=343, p. 3. (Letöltés ideje: 2018. 05. 15.). Ezzel kapcsolatban lásd még LEPRE i. m. p. 278.

15 Andreotti első kormánya 1972. február 17-én alakult meg, ám nem kapott parlamenti bizalmat, második kormánya 1972. június 26. és 1973. július 7. között irányította Olaszországot.

helyzettel. A miniszterelnök hangsúlyozta, hogy kormánya rövid időn belül jelentős erőfeszítésekkel fordul majd az ország belbiztonságának javítása érdekében. Erre szükség is volt, mert 1972. május 17-én ismét lecsapott a terror: milánói háza előtt gyilkolták meg Luigi Calabresi rendőrfelügyelőt, aki Giangiacomo Feltrinelli rejtélyes halála ügyében folytatott nyomozást[16].

„Giangi" Feltrinelli figyelemre méltó képviselője volt a hatvanas évek szélsőbaloldali olasz politikájának. A milliárdos könyvkiadót – az 1954-ben alapított *Giangiacomo Feltrinelli Editore* ma is az egyik legnagyobb könyvkiadó Olaszországban –, akit a mozgalomban „Osvaldo" néven ismertek, az évtized végére a nemzetközi kommunista mozgalomban a marxista tradíció és az új, fegyveres, magát forradalminak nevező baloldali irányzatok között tapasztalható törés miatt egyre inkább azon a véleményen volt, hogy a fegyveres harc, a „revolución" Olaszországban immáron elkerülhetetlen. Az 1926-ban született Feltrinelli túl fiatal volt ahhoz, hogy tevőlegesen részt vegyen az Ellenállás (Resistenza) fegyveres küzdelmeiben, és túl öreg, hogy forradalmár legyen – mondták róla. Ettől függetlenül a fegyveres harc mítosza nagy hatással volt rá, meggyőződésévé vált, hogy egy jobboldali államcsíny már csak idő kérdése, és hozzálátott a világháborút követően szélnek eresztett fegyveres csoportok (Gruppi d'Azione Partigiana) újjászervezésének egykori partizánok és fiatal forradalmárok toborzásával.[17] Annak ellenére, hogy kiváló kapcsolatokat ápolt az olasz kommunista párttal (Partito Comunista Italiano – PCI), később sokakkal egyetemben csalódott az PCI nem eléggé radikális politikájában, a szélsőségesek irányában találta meg politizálásának irányát.[18] Figyelemre méltó kapcsolatokkal rendelkezett a kubai és a csehszlovák kommunista rendszerek képviselőive. 1972. március 14-én halt meg egy balesetben, miközben saját kezűleg szeretett volna összeszerelni egy időzítő szerkezetet egy robbantásos szabotázsakcióhoz.[19] Sokan – nem minden alap nélkül – már a kortársak közül is politikai gyilkosságra gyanakodtak.[20]

Az PCI ez évben, a párt XIII. kongresszusán megválasztott főtitkárának véleménye megegyezett Feltrinelli elgondolásával a szélsőjobb megerősödése és egy jobboldali fordulat miatti nyugtalanság tekintetében. Ehhez a feszültséghez társult még az az érezhető riadalom, amelyet az 1973 őszi chilei események okoztak Enrico Berlinguer számára, aki precedensértékűnek ítélte meg Augusto Pinochet államcsínyét, és a Salvador Allende elnök hatalmát megdöntő puccs utáni tisztogatásokat. A hatalomátvétel során százak, és maga a baloldali elnök is életét vesztette, ezrek kerültek börtönbe, vagy tűntek el nyomtalanul. Berlinguer a dél-amerikai események mögött az Egyesült Államokat sejtette.

---

16 MALGERI, Francesco: I governi di Andreotti e la difficile democrazia degli anni Settanta in: Mario Varone-Ennio Di Nolfo (a cura di): Giulio Andreotti. L'uomo, il cattolico, lo statista Rubbettino 2010, pp. 152-153.

17 VESPA i. m. pp. 164-165

18 VESPA i. m. p. 165.

19 VESPA i. m. p. 166.

20 Feltrinelli szinte mindenki számára kényelmetlen szereplője volt ennek az időszaknak, jobboldali államcsínytől való félelme pedig megalapozott volt, halála sem baleset, hanem megrendezett gyilkosság volt,- vélte özvegye. http://www.rainews.it/dl/rainews/articoli/Inge-Feltrinelli-in-intervista-morte-mio-marito-fu-un-omicidio-politico-lui-sapeva-di-Gladio-bb10341e-7498-4139-b55e-723195612e34.html (Letöltés ideje: 2018. 05. 16.)

Egy jobboldali forgatókönyv megvalósulásától tartva Berlinguer három jelentős cikkben hívta fel a figyelmet a veszélyre a párt „*La Rinascita*" című politikai-kulturális lapjában. Utolsó írásában fontos gondolatokat megfogalmazva határozottan kiállt a katolikusok és kommunisták közötti „új és nagy történelmi megegyezés – nuovo e grande compromesso storico"[21] mellett, mindazon politikai erők megegyezéséért, akik összefogták és képviselték az olasz nemzet nagy többségének akaratát.[22] Az PCI vezetője minden egyeztetés, politikai előkészítés nélkül tette közzé javaslatát, ezzel nem csak és kizárólag a politikai oldal másik oldalán találhatókat lepte meg, hanem komoly fejtörést okozott saját kommunista párttársai, és a kommunista eszmékkel szimpatizálók körében is.

1.1. A történelmi kompromisszum (compromesso storico)

A régi-új gondolat, a koordinált és szoros együttműködés a kereszténydemokraták és a kommunisták között növekvő támogatást élvezett ugyan a kereszténydemokrata párt baloldalán, de egyáltalán nem nyerte el tetszését a párt – többek között Giulio Andreotti nevével fémjelzett – jobboldalán. Moro ezzel szemben úgy nyilatkozott, az idő tehát megérett arra, hogy megszűnjenek az PCI-t övező előítéletek. Ne feledjük, az PCI a második világháború végétől egészen 1947-ig kormányon volt.

Andreotti számára a „történelmi kompromisszum" nem volt több egy hibás gondolatnál, egy illuzórikus elképzelésnél.[23] Úgy vélekedett, hogy a „történelmi kompromisszum" nem más, mint egy Berlinguer által szorgalmazott és használt politikai trójai faló.[24] Olyan tragikus útként tekintett erre a formálódni látszó kompromisszumra-megegyezésre, amely tönkreteszi a kereszténydemokrata Olaszországot.[25] Véleménye szerint a „történelmi kompromisszum" egy mély ideológiai, kulturális, történelmi zűrzavar eredménye.[26] Ugyan szuggesztívnek tartotta a berlinguer-i elgondolást, de ezzel együtt alapvetően hibásnak. Olyan ötletnek, amely leginkább a kevéssé iskolázottaknak nyújt bizakodást, mondván: így legalább rend és nyugalom lesz az országban.[27] Fontos kiemelni, hogy a kommunistákkal ápolt jó viszony ellenére a rendszerszintű együttműködés ebben az időben elképzelhetetlen volt Andreotti számára, bár kiskaput, mint sokszor, ismét nyitva hagyott, 1974-ben arról beszélt: *„Ötven év múlva talán a dolgok megváltoznak."*[28] Andreotti stratégiai kérdésekben minden ellenkezés nélkül megfelelő feltételek mellett együtt tudott működni a kommunistákkal. Ezzel együtt a kérdésben megfogalmazott véleményét az is árnyalta, amelyről Oriana Fallaccinak nyilatkozott. Arról beszélt, hogy már a háborút követő időszakban megszületett benne az elgondolás, és kialakult azon meggyőződése, miszerint a demokrácia

---

21 BERLINGUER, Enrico: La crisi italiana. Scritti su Rinascita Editrice „l'Unità" S.p.A., 1985, p. 75.
22 Uo.
23 FRANCO, Massimo: Andreotti, Mondadori, 2008, p. 109.
24 Uo.
25 Uo.
26 Uo.
27 Uo.
28 Uo.

eszméje eredendően összeegyeztethetetlen a kommunizmussal. A személyes véleménye minden valószínűség szerint nagyban eltért politikusi értékítéletétől.[29]

Az 1975-76 évek fordulójára világossá vált, hogy a „középbal" politikai formáció nem működött már tovább, a rendszer az elmúlás jeleit mutatta. Az olasz kereszténydemokrata párt (Democrazia Cristiana – DC) az „előzés"[30] rémétől szinte bénultság állapotába merevedett. A kereszténydemokraták legfelsőbb vezetésében végrehajtott cserében látták a megoldást, ez azonban korántsem bizonyult elegendőnek, mert az PCI és Berlinguer vészesen növelte népszerűségét, a kommunisták ezekben az években történetük legjobb és legsikeresebb periódusát élték. Ezt természetesen mások is észrevették. A DC helyzetét mindezek mellett az sem könnyítette meg, hogy – a szélsőjobboldali terroristák mellett – immáron a szélsőbaloldali terroristák is aktivizálódtak: egyre kíméletlenebbül támadták az olasz állam képviselőit.

1976 februárjában a New York Times első oldalán feltűnt egy fénykép, amelyen a PCI főtitkára volt látható az SZKP XXV. kongresszusán mikor éppen a brezsnyevizmusssal történő szakításról és a „történelmi kompromisszum", vagy „demokratikus alternatíva" programszintű kinyilvánításáról beszélt.[31] Amennyiben mindez nem lett volna elég ahhoz a PCI előretörése miatt a DC-n belül egyre többen kezdjenek aggódni, ezekben a hetekben vált világossá egy parlamenti vizsgálóbizottság jelentéséből, hogy a CIA, az olaszországi amerikai nagykövteten, Graham Martinon keresztül bőkezűen finanszírozta az 1972-es parlamenti választások idején a mérsékelt pártok egyes képviselőjelöltjeit.[32] Az így kialakult helyzet a hetvenes évek közepén egyre nagyobb nyugtalansággal töltötte el a „történelmi kompromisszum" lehetősége miatt amúgy is aggódó Egyesült Államokat.

Andreotti és Henry Kissinger 1977. decemberi találkozója alkalmával az amerikai politikus a DC számára – egyfajta lehetséges megoldást felvázolva – új politikai szereplőkről („fresh faces"[33]) beszélt.[34] Az „előzés", a lehetőség, hogy Olaszország első pártja az évtizedes második szerepéből kilépő PCI legyen, rémálomként nehezedett az Egyesült Államok politikusaira. A múlt század ötvenes éveitől Itália egyre jobban felértékelődött az Egyesült Államok szemében. Politikai jelentősége geopolitikai helyzeténél fogva egyre fontosabbá vált az egymást követő amerikai adminisztrációk számára. Az Olaszországból érkező egyre több „aggasztó hír" hallatán az amerikaiak egyre többet fejezték ki rosszallásukat, arra pedig gondolni sem mertek, hogy szóba kerüljön a kommunisták kormányba emelésének gondolata. Az olasz politika számára a nyílt és/vagy burkolt politikai figyelmeztetések egyre gyarapodtak.

---

29 PANKOVITS i. m. p. 3.

30 Előzés, vagyis „*sorpasso*". A kifejezés a hetvenes évek Olaszországában a politikai kontextusban a két nagy párt a Democrazia Cristiana – DC, illetőleg a Partito Comunista Italiano – PCI közötti erőviszonyok utóbbi javára történő megváltozását jelentette (volna).

31 FRANCO i. m. p. 111.

32 Uo.

33 Uo.

34 Uo.

1976 nyarán a G7, vagyis az iparilag legfejlettebb országok képviselőinek találkozóját Porto Ricoban tartották. Olaszországot a kereszténydemokrata Aldo Moro kormányfő képviselte a tanácskozáson. Az újbóli intést az amerikaiak, angolok és franciák nevében a szociáldemokrata német kancellár, Helmut Schmidt kézbesítette, emlékeztetvén Olaszországot arra, hogy egyre növekvő aggodalom tapasztalható a tradicionális olasz politikáért, valamint arra, hogy a szövetséges államok növekvő nyugtalansággal figyelik az PCI kormányközelbe kerülésének lehetőségét.[35] Világossá vált, hogy veszélybe kerülhetnek az országnak addig biztosított financiális segélyek és kölcsönök, így pedig nehéz helyzetbe kerülhetett volna a nemzeti valuta is. Az amerikaiak többször megfedték az olasz politikusokat. Andreotti – akit a The New York Times nem minden ok nélkül nevezett az olasz politika De Gasperi utáni legérdekesebb emberének – úgy emlékezett, hogy Richard Gardner, az Egyesült Államok római nagykövete 1978-ban minden második hónapban jelezte, hogy most már igazán ne csússzanak tovább a kommunizmus irányába.[36]

A szintén jelentős kormányzati és kormányfői tapasztalattal rendelkező Aldo Moro ötödik kormánya 1976. február 12-től csak igen rövid ideig, 168 napig vezette az országot. A kabinet távozásával, az új választások kiírásával a kereszténydemokraták igazán kritikus helyzetbe kerültek, mert a rettegett „előzés" csakugyan kézzelfogható közelségbe került. Az előjelek semmi jóval nem kecsegtettek. A kedélyek felrázásán, az elégedetlen választók aktivizálásán kellett gondolkodni. A feladatot az ismert és elismert konzervatív újságíró Indro Montanelli vállalta. Az általa alapított „Il Giornale" című lap hasábjain fordult a – kormány és a kereszténydemokraták politikájával döntően elégedetlen – választók felé: „*Fogjátok be az orrotokat és szavazzatok a kereszténydemokratákra*!"[37], Mindeközben Berlinguer július 15-én, öt nappal a voksolás előtt a „Corriere della Sera" számára adott interjújában, ha lehet még jobban elbizonytalanította a választókat, mikor figyelemre méltó bejelentést tett: „*Azt akarom, hogy Olaszország ne lépjen ki az Atlanti Szerződésből… Nagyobb biztonságban érzem magam itt…*"[38] Ám még mielőtt olaszok milliói járulhattak volna az urnák elé, a Vörös Brigádok elrabolta és 1976. június 8-án meggyilkolta Francesco Coco vizsgálóbírót.[39] Sokan úgy vélik – és ezt nincs okunk kétségbe vonni –, hogy Mario Sosi, a Gruppo XXII Ottobre szélsőbaloldali terrorista csoport bírósági perében a vádat képviselő ügyész elrablása ügyében eljáró Coco meggyilkolása a Moro-ügy főpróbájának tekinthető.[40]

Az 1976 nyarán megtartott szavazás másnapjára a – kétségtelenül – győztes kereszténydemokraták tulajdonképpen föllélegezhettek, 38,7%-os eredményükkel megakadályozták, hogy a PCI – amely a szavazatok 34,4%-át szerezte meg[41] – végrehajtsa az „előzést". Andreotti ismételten a kormányfői szerep közelébe került, hiszen Moro kifejtette, hogy ezt a megtisztelő feladatot most nem ambicionálja.

---

35 VESPA i. m. Vespa ugyanitt Cossiga 2004-es kijelentésére hivatkozva közli, hogy Schmidt támogatta Olaszország NATO-tól történő eltávolítását egy számukra kedvezőtlen összetételű olasz kormány megalakulása esetén.

36 FRANCO i. m. p. 123

37 Uo. p. 113

38 Uo.

39 LEPRE i. m. p. 284.

40 Uo.

41 FRANCO i. m. p. 114.

Berlinguer a kormányalakítási tárgyalások alatt garanciákat szeretett volna Andreottitól, ő azonban, mielőtt bármire kötelezettséget vállalt volna, elérte az PCI-nél, hogy a párt továbbra is ismerje el és támogassa az olasz külpolitika két fundamentumát: az Atlanti Szerződést és az Európai Közösséget. Berlinguer ez elől nem zárkózott el. Berlinguer kérte Andreottit, hogy a támogatás fejében abban a pillanatban, ha az megszűnik, adja be lemondását. Erre Andreotti igenlő választ adott. Az ígéretét két évvel később, 1979-ben be is váltotta, mikor a PCI megvonta bizalmát a kormánytól.[42]

2. Aldo Moro elrablása

Ilyen politikai környezetben – a kommunisták, szocialisták, szociáldemokraták, republikánusok és liberálisok tartózkodása mellett – született meg Giulio Andreotti harmadik, „egyszínű" kereszténydemokrata kormánya[43]. A létrejött politikai formációt Andreotti egyik gazdasági tanácsadója, Luigi Cappuggi szellemes és találó megjegyzése nyomán az olasz politikában a „nem bizalmatlanság" (non sfiducia) kormányának szokták nevezni. Cappugi megjegyzése helytálló. Az Andreotti kormány megalakulását övező konszenzus nem a kabinetet támogató szavazatokban, hanem különleges és szokatlan módon a tartózkodó voksokban nyilvánult meg.[44] Ezzel kezdetét vette az a három esztendeig tartó időszak, amely „nemzeti szolidaritás" – „solidarietà nazionale" – éveiként vonult be a második világháborút követő időszak olasz politikatörténetébe.[45]

Az egymást követő kormányok legnagyobb belbiztonsági problémáját egyértelműen a terrorizmus, illetve a jelenségre adott válaszok jelentették. 1977-ben 2128 – átlagosan hatot naponta – terrorista merényletet követtek el Olaszországban, szemben a két évvel azelőtti 702 erőszakos cselekménnyel és az 1976-ban elkövetett 1198 merénylettel.[46] Az „ólomévek" legsúlyosabb, legnagyobb visszhangot kiváltó terrorista akciójára, arra az erőszakos cselekedetre, amellyel a terroristák valóban – ahogyan azt látni fogjuk megfogalmazták – az állam szíve ellen intézhettek támadást („colpire al cuore dello Stato"), 1978 tavaszán került sor. Március 16-án reggel, nem sokkal kilenc óra után Rómában a Vörös Brigádok elrabolta Aldo Moro kereszténydemokrata pártelnököt, volt kormányfőt és minisztert. A politikus ötfős testőrsége az emberrablás során életét vesztette (strage di via Fani). Morónak aznap a parlamentben kellett megjelennie, pártársa, Giulio Andreotti kormányának megalakulása miatti szavazáson.

A kérdés természetesen adódik, miért Moro?

---

42 VESPA i. m. p. 219. Ugyanitt Vespa közli, hogy Andreotti úgy látta, hogy Berlinguer döntését nagymértékben befolyásolta, hogy az Olasz Szociális Mozgalom néhány tagja 1977. január 13-án, Amintore Fanfani sugalmazására hagyta ott a pártot és fordult szembe Pino Rauti pártvezetővel. Az új parlamenti politikai formáció (Democrazia Nazionale Costituente di Destra) azonban továbbra is szorosan együttműködött a DC-vel.

43 http://giulioandreotti.org/it (Letöltés ideje: 2018. 05. 15.)

44 MALGERI i. m. p. 164.

45 Uo.

46 VESPA i. m. p. 184.

A fő célpont nem is ő volt. Aldo Moro, a Kereszténydemokrata Párt elnöke a szokások rabja volt, olyan mindennapi elfoglaltságai voltak, amelyek sokkal könnyebben megközelíthetővé tették őt a Vörös Brigádok számára, mint a többi lehetséges célpontot. A szélsőbaloldali terrorszervezet ugyanis több más fontos politikus elrablását is vizsgálta ezekben az években. Célkeresztjükben szerepelt Amintore Fanfani szenátusi elnök, a belügyminiszter, Francesco Cossiga – a Vörös Brigádok számára csak „K" – vagy a kijelölt kormányfő, Giulio Andreotti[47]. Cossiga azt írta visszaemlékezéseiben, hogy igazi céljuk Andreotti volt, ám ő folyamatosan változtatta testőreivel a napi rutinfeladatokat. Nem volt állandó útvonala, hogy lakásából eljusson az irodájába, onnan pedig a parlament épületébe. Moro elrablása technikai értelemben sokkal könnyebbnek mutatkozott, végül a Vörös Brigádok terroristái őt választották.[48] De vajon kik voltak ezek a terroristák, és valójában hogyan nézett ki a mindazon ideológiai háttér, aminek mentén szerveződtek?

2.1. A Vörös Brigádok (Brigate Rosse)

1970-ben a Vörös Brigádok első sejtjei vegyes társadalmi háttérrel bírtak és összességében ez az ideológiai heterogenitás továbbra is jellemző maradt a terrorszervezetre. Voltak, akik gyári munkásfelkelések tapasztalataival (Sit-Siemens, Milánó) a hátuk mögött csatlakoztak, de voltak olyanok is, akik az egyetemi tanulmányaik alatt jutottak el arra a felismerésre, hogy az állam elleni fegyveres harc elkerülhetetlen. Ilyen volt többek között a trentói egyetem szociológiai karán formálódó szárny, a Renato Curcio és Margherita „Mara" Cagol nevével fémjelzett, az 1968-as diákmozgalmakhoz és a katolikus formációkhoz kötődő egyetemi csoport. [49]

Az évtized első időszakában több parlamenten kívüli baloldali csoport is a radikális utcai tiltakozásokkal, gyárfoglalásokkal, egyetemi blokádokkal nyomatékosította véleményét, de ezek az akciók nem léptek túl egy bizonyos határt. A radikalizálódó baloldali csoportok és az egyre jobban magára találó Brigate Rosse (Vörös Brigádok)-sejtek között az alapvető különbség abban mutatkozott, hogy utóbbiak pontosan a terrorizmust, az erőszakot és a fegyveres harcot választották, mint végső eszközt politikai céljaik elérése érdekében.

Az országban a hetvenes évekig a létező terrorizmus egyetlen fajtáját a szélsőjobboldali szervezetek akciói jelentették. Különösen aktívak korábban és akkor a Squadre azione Mussolini, az Ordine Nuovo vagy a Terza Posizione elnevezésű szélsőjobboldali terrorista szervezetek és csoportok. Az Ordine Nuovo terrorszervezet volt a felelős az „Italicus" expressz 1974-es felrobbantásáért, melynek következtében tizenketten életüket vesztették.

1970-től a Vörös Brigádok megkezdte a proletariátus felszabadítása érdekében végzett „fegyveres propagandáját", amely közel négy esztendeig tartott. A terrorszervezet azután 1974-ben már egy új, alapvető jelentőségű brosúrában –

---

[47] COSSIGA, Francesco: La versione di K Sessant'anni di controstoria RAI ERI-Rizzoli, 2009, p. 113

[48] Uo. lásd még GRASSI, Antonello – SANTORO, Gianpaolo: Giulio. La storia di Andreotti dalla A alla Z Edizioni CentoAutori, 2013, pp. 46-47.

[49] LEPRE i. m. p. 278.

„Contro il neogollismo portare l'attacco al cuore dello Stato"[50] – definiálta újra magát és pontosította politikai céljait. Deklarált célja lett ettől kezdve a gazdasági krízis és a társadalmi feszültségek következményeit kezelni és orvosolni nem tudó állam központja – láttuk, a „szíve" – elleni támadások előkészítése, és végrehajtása, a rendszer elpusztítása. A kereszténydemokraták, és a vele „kiegyező" baloldali pártok is a Vörös Brigádok célpontjaivá váltak: megjelent az emberrablásokban és/vagy gyilkosságokban kifejeződő szélsőbaloldali terrorizmus. 1975 áprilisában azután újabb krédóját ismertette meg a Vörös Brigádok: multinacionális és imperialista államról beszélt, és arról, hogy ez ellen most már a rendszer szívében, a városokban kell küzdeni, tehát tovább kell folytatni a városi gerillaharcokon keresztül az állam szíve elleni fegyveres támadásokat.51

Róma válasza nem késett sokáig: 1974 és 1977 között tömeges letartóztatásokat foganatosítottak. Carlo Alberto Dalla Chiesa52 tábornok vezetésével az olasz állam szervei egyre nagyobb mértékben és sikeresen mértek csapást a Vörös Brigádokra. 1976-ban többek között rendőrkézre került a Vörös Brigádok alapítói közül Renato Curcio és Alberto Franceschini. A terrorszervezet mindezen kemény csapások ellenére azonban még tovább élt és létezett, sőt ebben az évben 2128 terrorista akciót hajtott végre a két évvel azelőtti 705-höz, és az 1976-os 1198-hoz képest53. Továbbra is bírókat, ügyészeket, ügyvédeket, vagyis az állam képviselőit vette célba, majd az újságírók ellen is fordult54.

2.2 Moro fogsága és kivégzése

Moro elrablása és meggyilkolása akkor következett be, mikor az ország elmozdulni látszott a politikai bénultság állapotából. 1978. március 16-án maga Moro is a parlamentbe készülődött, hogy leadja szavazatát Andreotti kereszténydemokrata kormányának parlamenti vitájában. Aznap este a kormány mind a képviselőházban lefolytatott vitán, mind pedig a szenátusi bemutatkozás alkalmával kiállta a próbát. Előbbiben 545 igen, 30 nem szavazat mellett, az utóbbiban 267 igen szavazattal a 272 szavazóból kapta meg a parlamenti képviselők bizalmát.[55] Andreotti kormányt alakíthatott.

Moro 55 napig volt a Vörös Brigádok foglya. A rabságban lévő politikus elleni „per" 1978. március 25-én kezdődött, aki négy nappal később, március 29-én levélben fordult a belügyminiszterhez és a kormányhoz, hogy kezdjenek tárgyalást a Vörös Brigádokkal. A DC azon szárnya, amelyhez Andreotti is tartozott, a Vörös Brigádokkal kapcsolatban az erélyesség pártjára állott. Az általa elfoglalt politikai álláspont szerint a terroristákkal nem szabad tárgyalni, nem lehetett tárgyalni (strategia della fermezza). E politikai állásfoglalást osztotta még a DC Benigno Zaccagnini vezette szárnya, a PCI, a republikánusok. Ez az álláspont alapvetően szembenállt mindazzal, amit egy másik oldal, az úgynevezett „tárgyalás" képviselői

---

50 LEPRE i. m. p. 280.
51 Uo.
52 Carlo Albero Della Chiesa tábornok miután az állam képviseletében sikeresen harcolt a Vörös Brigádok ellen, 1982-ben a szicíliai maffia áldozata lett.
53 VESPA i. m. p. 184.
54 Leghíresebb áldozatuk Indro Montanelli volt, akit 1977. június 3-án sebesített meg a Vörös Brigádok Walter Alasia hadoszlopa.
55 MALGERI i. m. p. 194.

vallottak. Bettino Craxi szocialistái, a radikálisok és a kereszténydemokraták kisebbségi képviselői elgondolása szerint Moro élete megmenthető, és éppen ezért mindent meg kell is tenni annak érdekében, hogy a politikus kiszabaduljon fogságából (strategia dela trattativa).

Andreotti szerint az elutasítás politikája két összetevőből született. Az egyik, a politikai, az olasz kommunista párthoz kapcsolódott. A terrorszervezet propagandájának egyik PCI-val kapcsolatos alapvetése ugyanis az volt, hogy az olasz kommunisták árulók, 1947-től egészen 1976-ig minden alkalommal az aktuális kormány ellenében szavaztak, de ez alkalommal elárulták választóikat, elfogadták az Andreotti kormány politikai célkitűzéseit, az atlanti és az európai politikát. Ezzel tehát ezt az irányvonalat kellett valamilyen módon óvni, megvédeni. A másik oka pedig az volt, hogy rendkívül fenyegetett helyzetben találta magát az olasz állam, a szélsőbaloldali terror állami képviselők ellen intézett támadásokat. Andreotti szerint a via Fani és via Stresa kereszteződésénél történteket követően komoly ellenkezéssel kellett volna számolnia, ha az olasz állam engedett volna a zsarolásának.[56] Andreotti később azt is felidézte, hogy Moro testőrségét alkotó fegyveresek egyikének özvegye telefonált a miniszterelnökségre: *„ha engednek, közölte velünk egy buddhista szerzeteshez hasonlóan gyújtom fel magam a Piazza Colonnán.* (A Miniszterelnökség palotájának otthont adó tér Rómában-A.G.)"[57] Leszögezte, hogy nem az állam presztízsét védték, csupán arra ügyeltek, hogy az intézmények működőképességét biztosítsák.[58] Ám mégis meg kellett őrizni az állam méltóságának és cselekvőképességének látszatát: a terroristák egyszerű bűnözők, hogyan lehetne bűnözőkkel tárgyalni. Az sem látszott valószínűnek, hogy az PCI hajlandó önálló politikai entitásként elismerni a Vörös Brigádokat.

VI. Pál pápa több alkalommal személyesen fordult a terroristákhoz a kereszténydemokrata politikus szabadon bocsátása érdekében. Sikertelenül. A terrorszervezet halálra ítélte a politikust. A terroristákkal történő tárgyalás kisebbségi véleményét többek között a szocialista Bettino Craxi képviselte, sőt egy 2006-ban megjelent életrajza egyenesen úgy fogalmazott, hogy rajta kívül *„igazán senki újját nem mozdította."*[59] A kereszténydemokraták és az olasz kommunisták nem tágítottak a „strategia della fermezza" politikájától, annak ellenére sem, hogy fogságából Moro többször jelezte: a fogolycsere az egyetlen járható út, az olasz állam nem kezdte meg a tárgyalásokat a Vörös Brigádokkal. Április 23-i keltezésű az a levél, amelyet a fogságban lévő Moro a kereszténydemokraták parlamenti frakcióvezetőjének, Flaminio Piccolinak címzett. Ebben Andreotti politikáját bírálva így ír: *„Ami fontos, meggyőzni Andreottit, hogy nem a győztes utat követi […] Érdemes tárgyalni."*[60] Aldo Moro-t 1978. május 9-én kivégezték. Holttestét az olasz főváros egyik forgalmas utcájában egy Renault 4-es személygépkocsi

---

56 VESPA i. m. p. 198.
57 Uo.
58 Uo.
59 CATANIA, Enzo: Bettino Craxi. Una storia tutta italiana Boroli Editore Milano, 2005, p. 93
60 Moro levele Piccolinak, 1978. április 23. in: Michele Di Sivo (a cura di): La lettere di Aldo Moro dalla prigionia alla storia, Direzione Generale per gli Archivi, Archivio di Stato di Roma, 2013. http://151.12.58.123/dgagaeta/dga/uploads/documents/FuoriCollana/539a8ce3a0109.pdf (Letöltés ideje: 2018. 05. 05.)

csomagtartójában találták meg, félúton a kommunista párt és a kereszténydemokraták székháza között.

A kereszténydemokrata politikus halála országos felháborodást és gyászt váltott ki szerte Olaszországban. Az emberek még azelőtt az utcákra és terekre vonultak, mielőtt a szakszervezeti vezetők meghirdették volna a Moro elrablása és halála miatti országos sztrájkot. Andreotti később bevallotta: komolyan aggódtak egy mindent elsöprő országos forradalom lehetősége miatt.[61]

Milyen szerepe volt Andreottinak az úgynevezett Moro-ügyben? Az eltelt évtizedek alatt számtalanszor próbáltak válaszolni a kérdésre. A DC elnökének halála hatalmi játszmák bonyolult szövevényeinek, párhuzamoknak és kereszteződéseknek az eredménye. Sandro Provvisionato és Ferdinando Imposimato három évtizeddel Moro halálát követően megjelent könyvükben[62] több fontos kérdést tesznek föl a mai napig megnyugtatóan nem lezárt ügyben. A szerzőpáros arra a konklúzióra jutott, hogy Moro-nak „meg kellett halnia”[63], sorsa a fogsága idején már több is volt, mint elrendeztetett, az nem a rendőrség – egyébként valóban tapasztalható – tehetetlensége, hanem a DC legfelsőbb vezetését (Andreotti, Cossiga) érintő tudatos politikai döntés eredménye, amely ellen sem az Egyesült Államoknak, sem pedig a Szovjetuniónak nem volt érdemi ellenvetése.[64] A könyvben a szerzők sorra teszik fel a zavarba ejtő kérdéseiket a Moro-üggyel kapcsolatban. Ezek egyike az 1978. január 31-én belügyminiszteri rendelettel létrehozott különleges belügyi egységre az UCIGOS-ra (Ufficio Centrale Investigazioni Generali e Operazioni Speciali) vonatkozott. Az egyfajta titkosszolgálati egységként működő szervezet – amelynek vezetője jelentési kötelezettséggel nem a rendőrség vezetőjének, hanem közvetlenül a belügyminiszterhez tartozott[65] – volt ugyanis az egyetlen, amely nyomozati munkát látott el Moro fogsága alatt, míg például Carlo Alberto Dalla Chiesa csendőr tábornok, vagy Emilio Santillo vizsgálóbíró a „kispadon várakoztak”[66].

Az „ólomévek” legsúlyosabb terrorcselekményére 1980. augusztus 2-án 10 óra 25 perckor Bolognában került sor. A város vasúti főpályaudvara előtt robbantottak gyilkos erejű pokolgépet az újfasiszta Nuclei Armati Rivoluzionari (NAR) terroristái. A merénylet során 85 személy életét vesztette, 200 fő sebesült meg súlyosan. Hat nappal később, az áldozatok temetésén megjelent Sandro Pertini köztársasági elnök és a város polgármestere, Renato Zangheri. A tömeg igazságot, a felelősök megnevezését és megbüntetését követelte. A bíróság

---

61 VESPA i. m. p. 193.

62 Sandro PROVVISIONATO – Ferdinando IMPOSIMATO: Doveva morire. Chia ha ucciso Aldo Moro. Il giudice dell”inchiesta racconta. Chiarelettere, 2008.

63 „Doveva morire”, vagyis „Meg kellett halnia” a címe Adriano Botta újságíró a „L’Europeo” című hetilap 2009/11-es számában Sandro Provvisionatóval, az egyik szerzővel készített interjújának.

64 Uo. p. 107

65 Uo. p. 108

66 Uo. p. 109.

azonban csak 1995. november 23-án hozott ítéletet, amelyben Valerio Fioravantit és Francesca Mambrót, a NAR terroristáit életfogytiglani börtönbüntetésre ítélte.[67]

Összegzés

Giulio Andreotti 1972 és 1979 között öt alkalommal állt az olasz kormány élén. Ez az időszak nagymértékben hozzájárult ahhoz, hogy Andreotti jelentős, az olaszok kívánságait meghallgató, polgártársait értő rugalmas politikusként jelenjék meg milliók szemében. A szerep, amelyet ezekben az években Moro mellett, majd annak halálát követően egyedül fölvállalt, hozzájárult ahhoz, hogy az olasz társadalom sikeresen megbirkózzon a hetvenes évekkel, hogy Olaszország eljusson a kilencvenes évekig, az „első köztársaság" végéig. Elképzelései és a politikája nem csekély mértékben járult hozzá ahhoz, hogy az olasz társadalom viszonylagos épségben jutott el a kilencvenes évekig. Akkor azonban összeroppant a „mani pulite" („tiszta kezek") korrupciós botrány nyomása alatt. Ettől függetlenül a „Révész" szerepe elvitathatatlan. Sokan gondolják úgy, hogy ennek az izgalmas időszaknak a miértjeit, az ok és okozati összefüggéseket sohasem fogjuk megismerni, kérdéseinkre soha nem fogunk kimerítő választ kapni. Azoknak, akik így vélekednek, alighanem igazuk van: az eddig elmondottakon kívül számos rejtély vár még megoldásra: az 1980-as usticai katasztrófától a maffia és az állam kapcsolatán át a P2 szabadkőműves botrányig bezárólag.

Szokatlan és talán nem feltétlenül szerencsés egy tudományos munka összegzésében egy játékfilm sorait idézni, az abban elhangzottakra utalni. Most mégis megtesszük, mert fontosnak tartjuk Paolo Sorrentino 2008-ban rendezett játékfilmjét Giulio Andreotti életéről. Ennek a filmnek kiemelkedő jelenetében a Giulio Andreottit játszó Tony Servillo szerepe szerint fiktív monológban szól a hetvenes évek politizálásáról és következményeiről:

„…Meggyónom, hogy az én bűnöm volt, az én bűnöm, az én rettentő bűnöm. Ezt mondom majd, még ha nincs is értelme: a pusztulás, ami szétzilálta az országot és kiprovokálta a terrort, amire izolálni lehet a szélsőséges pártokat és megerősíteni a centristákat, mint amilyenek a kereszténydemokraták, ezt úgy jellemezték, hogy feszültség stratégia, pedig helyesen inkább túlélési stratégia. Roberto, Michele, Giorgio, Carlo Alberto, Giovanni, Mino, a drága Aldo, munka miatt, vagy szükségszerűségből mind az igazság hajthatatlan szerelmesei. Mindegyik bomba, amelyik csendre lett hatástalanítva, készen áll, hogy felrobbanjon. Mind azt hiszik, hogy az igazság a helyes dolog, pedig valójában az a világ vége, és nem engedhetjük meg, hogy vége legyen a világnak valami helyes dolognak a nevében.
Feladatunk van, isteni feladatunk, nagyon kell szeretnünk Istent, hogy megértsük, hogyan szolgálja a jót a szükséges gonosz…Isten tudja ezt, és én is…én is tudom."[68]

---

[67] https://www.corriere.it/tecnologia/domande-google/notizie/cosa-successo-google-2-agosto-1980-strage-stazione-bologna-depistaggi-processi-56585ab6-76ef-11e7-891a-91d906aac00b.shtml (Letöltés ideje: 2018. 05. 17.)

[68] Il divo (A megfoghatatlan) – Paolo Sorrentino filmje, 2009 (Lucky Red/Best Hollywood)1:12.00'-1:13:50'

Felhasznált irodalom:

- BERLINGUER, Enrico: La crisi italiana. Scritti su Rinascita Editrice „l'Unità" S.p.A., 1985
- CATANIA, Enzo: Bettino Craxi. Una storia tutta italiana Boroli Editore Milano, 2005
- COSSIGA, Francesco: La versione di K Sessant'anni di controstoria RAI ERI-Rizzoli, 2009
- DI SIVO, Michele (a cura di): Le lettere di Aldo Moro dalla prigionia alla storia. in: http://151.12.58.123/dgagaeta/dga/uploads/documents/FuoriCollana/539a8ce3a0109.pdf (Letöltés ideje: 2018. 05. 05.)
- FRANCO, Massimo: Andreotti, Mondadori, 2008
- FRANZINELLI, Mimmo: RSI. La repubblica del duce 1943-1945 Oscar Mondadori, 2011
- GRASSI, Antonello – SANTORO, Gianpaolo: Giulio. La storia di Andreotti dalla A alla Z Edizioni CentoAutori, 2013
- Aurelio LEPRE: Storia della prima Repubblica. L'Italia dal 1943 al 2004. il Mulino, 2004.
- MALGERI, Francesco: I governi di Andreotti e la difficile democrazia degli anni Settanta in: Mario Varone-Ennio Di Nolfo (a cura di): Giulio Andreotti. L'uomo, il cattolico, lo statista Rubbettino 2010, pp. 145-205
- MARLETTI, Carlo: Uccidere in nome delle idee Continuità e mutamenti del terrorismo ideologico e politico degli anni settanta e ottanta in: http://www.fondazioneveranocentini.it/index.php?option=com_content&view=article&id=139:uccidere-in-nome-delle-idee&catid=67&Itemid=343 (Letöltés ideje: 2018. 05. 15.)
- PANKOVITS József: Giulio Andreotti (1919-2013) in: http://www.grotius.hu/doc/pub/APKQRJ/2013-08-05_pankovits_jozsef_andreotti.pdf (Letöltés ideje: 2018. 05. 11.)
- PROVVISIONATO, Sandro – IMPOSIMATO, Ferdinando: Doveva morire. Chia ha ucciso Aldo Moro. Il giudice dell"inchiesta racconta. Chiarelettere, 2008.
- VESPA, Bruno: Storia d'Italia da Mussolini a Berlusconi. Mondadori Rai, 2004. p. 165.
- http://www.giulioandreotti.org
- http://www.memoria.san.beniculturali.it/
- http://www.piantiamolamemoria.org/strage-di-peteano/
- http://www.rainews.it
- https://www.youtube.com/

TÓTH TAMÁS

AZ EURÓPAI UNIÓ TERVEZETT KIBERBIZTONSÁGI TANÚSÍTÁSI KERETRENDSZERÉNEK BEMUTATÁSA[1]

Bevezetés

Az információs társadalom globalizációja okán az IT-rendszerek és -hálózatok az Európai Unió társadalmi és gazdasági alrendszereinek a gerincét képezik. A legtöbb ágazat mára digitális technológiák alkalmazása nélkül nem lenne képes a hatékony működésre. Az ágazatokban alkalmazott, hálózatba kötött intelligens IT-eszközök képesek a számukra releváns információkat detektálni, valamint ezeket megosztani. Ezen intelligens digitális eszközök alkotják a dolgok internetét (IoT[2]), mely méretét és jelentőségét tekintve rendkívül gyors ütemű fejlődés előtt áll. Az intelligens eszközök elterjedése, a hálózatok folyamatos bővülése azonban veszélyeket rejt magában. Egy eszköz biztonsági réseinek kihasználásával a hálózat minden eleme, valamint a kapcsolódó hálózatok is elérhetővé válhatnak egy károkozó számára, így a helyi támadás globális szintre eszkalálódhat, hatalmas károkat okozva tagállami, uniós vagy akár globális szinten. Az Európai Unió felismerte az IoT térnyerését, az okos eszközök iránti fogyasztói kereslet jövőbeli növekedését, globális elterjedését, így szükségesnek látta hatásvizsgálatban felmérni a termékekben rejlő és használatuk során felmerülő biztonsági kockázatokat. A *SWD(2017) 500 FINAL*[3] számú hatásvizsgálat munkadokumentumát az Európai Bizottság 2017. szeptemberére készítette el. A hatásvizsgálat további célja előkészíteni egy, az uniós kiberbiztonságra vonatkozó jogszabály megalkotását, melyben az ENISA[4] 2020-ban lejáró megbízatását is felülvizsgálni kívánja, valamint az IKT-termékek, -szolgáltatások és -folyamatok uniós szintű kiberbiztonsági

---

1 A publikáció az Európai Bizottság IKT-termékek kiberbiztonsági tanúsításáról szóló SWD(2017) 500 final számú hatásvizsgálat 4/6. és 6/6. munkadokumentumának a tervezett, uniós szintű kiberbiztonsági tanúsítási keretrendszerről szóló részeit kívánja összefoglalni és ismertetni.

2 Internet of Things.

3 COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). - BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM HATÁSVIZSÁLGAT, amely a következő dokumentumokat kíséri Összefoglaló Jelentés AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az Európai Uniós Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály"). SWD/2017/0500 final 2017/0225 (COD), Európai Bizottság, Brüsszel, 2017. szeptember 13., https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52017SC0500 (Letöltés ideje: 2018. 07. 22).

4 European Agency for Network and Information Security – Európai Uniós Hálózat- és Információbiztonsági Ügynökség.

tanúsítási keretrendszerét hivatott szabályozni és deklarálni, a kibertámadásokkal szembeni ellenálló képesség fokozása érdekében. E publikáció az IKT[5]-termékek tanúsítási eljárásainak kockázatait felmérő, valamint a biztonságos eljárások kidolgozása érdekében, tanúsítási szakpolitikai javaslatokat megfogalmazó idegen nyelvű dokumentációt kívánja lényegre törően összefoglalni és értékelni magyar nyelven.

1. A hatásvizsgálat elkészítésének előzményei

Az EU-n belül is a kibertbiztonságot veszélyeztető incidensek száma egyre növekszik, amely jelentős gazdasági károkat okoz mind az állami, mind pedig a magánszektor szereplői számára. Emellett jelentős negatív társadalmi hatással is jár, mivel az állampolgárok digitális világba vetett bizalmának megrendülését eredményezi. A támadások hatékony kezelése, illetve minimalizálása érdekében a Bizottság Kiberbiztonsági Munkacsoportja felül kívánja vizsgálni az ENISA megbízatását, annak érdekében, hogy a tagállamok kiberbiztonsági ellenállóképességét fenntartható szintre növeljék, számításba véve a „Hálózati és információs rendszerek biztonságról szóló irányelvet”[6] (NIS Direktíva), továbbá „Az Európai Unió általános adatvédelmi rendeletét” (GDPR)[7] a kollektív fellépés érdekében. Megjelent számos nemzeti kezdeményezés is annak érdekében, hogy magas szintű biztonsági követelményeket állítsanak az IKT-összetevőkkel szemben. Ezek azonban hatalmas kockázatot hordoznak magukban, mivel széttagolttá teszik a tanúsítási rendszereket, valamint a digitális egységes piacot (DSM[8]), mely azt mutatja, hogy a kollektív ellenálló képesség a tagállamok által hozott egyedi intézkedések szintjén nem növelhető. A NIS Direktíva értelmében a meghatározó ágazati szereplők, például az energiaipari, a közlekedés- és vízügyi, a banki szolgáltatók, a pénzügyi piaci infrastruktúra, az egészségügyi és a digitális infrastruktúra szereplői, valamint a digitális szolgáltatók kötelesek intézkedéseket tenni a biztonsági kockázatok megfelelő kezelése érdekében. Az IKT-termékek és -szolgáltatások tanúsítási rendszereinek jelenlegi összehangolatlansága a tagállamokra nézve jogilag kötelező erejű és hatékony közös keretprogram hiányából is adódik. Ez egy nem kellő biztonsággal működő, széttagolt, aszimmetriákkal rendelkező piacot eredményez, melyben a szereplők nem tudják csökkenteni a támadások okozta többletköltségeik mértéket, nem tudják fokozni termékeik és szolgáltatásaik vonzerejét, így elmarad a tervezett növekedés. A

---

5 ICT – Information and communications technology – Információs és kommunikációs technológia.

6 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, Európai Parlament és Tanács, Brüsszel, 2016. július 6., https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=EN (Letöltés ideje: 2019. 02. 14.)

7 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, Európai Parlament és Tanács, Brüsszel, 2016. április 27., https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Letöltés ideje: 2019. 02. 14.)

8 Digital Single Market.

Bizottság ezek hatására dolgozott ki egy lehetséges európai IKT-biztonsági tanúsítási keretrendszerre vonatkozó javaslatot, valamint értékelte megvalósíthatóságát és hatásait.

2018. december 10-én az Európai Parlament, a Tanács és az Európai Bizottság politikai megállapodásra jutott a „Kiberbiztonsági jogszabály"-ról, mely értelmében az ENISA átalakításával, megbízatásának meghosszabbításával, valamint feladatainak optimalizálásával támogatni kívánják a tagállamokat a kiberbiztonsági fenyegetésekkel és támadásokkal szemben. Az ENISA-t egy független szakértői központtá kívánja átszervezni az uniós jogalkotó, mely képes lesz fokozni a polgárok és a versenyszféra szereplőinek biztonságtudatosságát, továbbá támogatja az EU intézményrendszerét és tagállamait a normák megalkotásában és végrehajtásában. A szervezet fokozná a tagállamok kibertámadások elleni hatékonyabb fellépését, a szélesebb körű együttműködés és az uniós szintű koordináció területén. A jogszabály kialakítaná az Európai Unió kiberbiztonsági tanúsítási keretrendszerét is a célból, hogy erősítse az online szolgáltatások és felhasználói termékek kiberbiztonsági képességeit. Az uniós normatíva által kialakított keretrendszer elvárásokat fog meghatározni a nemzeti szintű európai kiberbiztonsági tanúsítási rendszerek létrehozásához.

Az uniós jogszabálytól pozitív hatást várhatnak mind az EU-s polgárok, mind pedig a versenyszféra szereplői egyaránt. A törvény által fokozható lesz az állampolgárok bizalma a mindennapi használatban lévő IKT-eszközeikkel kapcsolatban, egy egységes, a biztonságot garantáló tanúsítási keretrendszernek köszönhetően. Az uniós szintű IKT-tanúsítási keretrendszernek további előnye, hogy a tanúsítványok egyetemlegesen érvényesek lesznek az Európai Unió összes tagállamában, így nem lesz szükséges a tagállamokban külön-külön a nemzeti vagy lokális eljárások lefolytatására, amely megoldást kínálhat a piac jelenlegi széttagoltságára. Ez ösztönözheti a gazdasági társaságokat IKT-termékeik kiberbiztonságba történő beruházásra, mivel az uniós szintű tanúsítási keretrendszer alkalmazásával sokkal szélesebb piacra léphetnek ki termékeik és szolgáltatásaik, így versenyelőnyben lesznek a szűkebb piaccal rendelkező versenytársaikkal szemben.[9]

2. A tanúsítási eljárások ismertetése

Valamely termék, szolgáltatás vagy folyamat tanúsítása biztosítékot jelent arra, hogy az megfelel a hatályos jogszabályoknak, az előírt szabványoknak, továbbá szerződésekben meghatározott egyéb dokumentumoknak.[10] *„A tanúsítás, amely a termékek, szolgáltatások és folyamatok független és akkreditált testület általi meghatározott, szabványos kritériumokon alapuló formális értékeléséből és egy*

[9] EU negotiators agree on strengthening Europe's cybersecurity, Cybersecurtiy Act, Európai Bizottság, Brüsszel, 2018. december 11. https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en (Letöltés ideje: 2019. 02. 17.)

[10] SZŐKE Gergely László: Az önszabályozás, audit és tanúsítás lehetőségei és korlátai az adatvédelem területén, Infokommunikáció és jog 2014. XI. évfolyam 1. szám, HVG-Orac Kft., Budapest, 2014. p. 16., https://infojog.hu/wp-content/uploads/pdf/201457_SzokeGergelyLaszlo.pdf (Letöltés ideje: 2019. 02. 16.)

megfelelőségi tanúsítvány kiállításából áll, fontos szerepet játszik abban, hogy javuljon a termékek és szolgáltatások biztonsága és nőjön a beléjük vetett bizalom."[11] Az IKT-termékek vonatkozásában kialakítandó egységes tanúsítási keretrendszer célja, hogy javuljon a termékek és szolgáltatások, folyamatok biztonsága, tájékoztatást és garanciát nyújtson az állampolgárok számára az infokommunikációs technológiák biztonsági tulajdonságairól, így növelve a beléjük vetett bizalmat. Ez a folyamat hosszútávon pozitív hatást gyakorolhat, azaz az IKT piaci fellendülését okozhatja.[12]

A tanúsítás a kezdeményezéssel kezdődik, mely során a fejlesztő kezdeményezi a termék bevizsgálását az illetékes tanúsító szervezetnél. Ezt követi az értékelés végrehajtása, mely háromféleképpen történhet. A vállalat öntanúsítást végez, egy a vállalathoz köthető részleg végzi az értékelést, továbbá harmadik fél hajtja végre az eljárást. Az utóbbi két esetben a döntés meghozatalának eredményeképpen kapja meg a termék a megfelelő tanúsítványt. A felügyeleti szakaszban lehetőség nyílik a periodikus ellenőrzésre annak érdekében, hogy biztosítsák a tanúsítvány aktualitását, valamint kezdeményezhessék új eljárás lefolytatását.[13]

1.	**Kezdeményezés**	Kapcsolatfelvétel, igényfelmérés
		Árajánlat és szerződéskötés
2.	**Értékelés végrehajtása**	Auditor(ok) kijelölése
		Előaudit (Opcionális)
		Dokumentáció felülvizsgálata és audit tervezése
		Helyszíni audit lefolytatása
		Jelentés készítése
3.	**Tanúsítvány kiállítása**	Tanúsítvány kiállítása
4.	**Felügyeleti szakasz**	Felülvizsgálati audit
		Tanúsítvány megújítása

1. ábra: A tanúsítási eljárás folyamata
saját szerkesztés[14]

[11] Javaslat, AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az Európai Uniós Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály"). COM(2017) 477 final/3 2017/0225 (COD),Európai Bizottság, Brüsszel, 2018. február 22., https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN, p. 10. (Letöltés ideje: 2019. 02. 17.)

[12] BENCSIK Balázs: A kiberbiztonsági feladatok kezelése az európai uniós jogalkotás fényében, Belügyi Szemle 2019. LXVII. évfolyam 1. szám, Belügyminisztérium, Budapest, 2019. pp. 99-100.

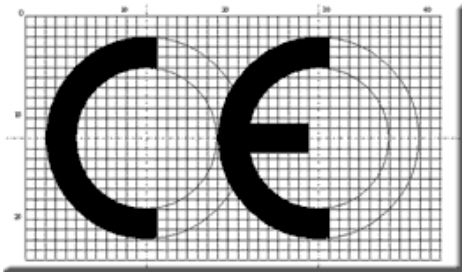
[13] DR. GREGÁSZ Tibor: A minőségirányítás alapjai Szabványos minőségmenedzsment rendszerek működési elvei, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, NKE, Budapest, 2014, https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/a-minosegiranyitas-alapjai.original.pdf, p. 42. (Letöltés ideje: 2018. 08. 10.)

[14] A tanúsítás folyamata, Eurpoean CERT, http://www.european-cert.hu/ (Letöltés ideje: 2019. 02. 16.)

A tanúsításoknak alapvetően négy tárgya lehet:

Terméktanúsítás során egy erre feljogosított szervezet a beküldött termék típusvizsgálata és dokumentációja alapján nyilatkozik annak szabvány, vagy jogszabály szerinti megfelelőségéről. A termékbiztonsági szempontú tanúsítás lehet kötelező, de léteznek önkéntesen vállalt termék-megfelelőségi tanúsítások is. A tanúsítási eljárást a legtöbbször egy adott tanúsító cég végzi. Az eljárásnak és az ezt igazoló címke használatának jelentősebb költségvonzata lehet. A leggyakoribb terméktanúsítás az EU-ban a termékbiztonságot szolgáló, új megközelítésű direktívák hatálya alá tartozó, fokozott biztonsági kockázattal bíró[15] termékkörben kötelezően megszerzendő „CE" jelölés.

A jelölés, vagy más néven a címkézés egy igen fontos eleme a tanúsítási eljárásnak, hiszen a címkéken keresztül tájékoztatható a fogyasztó, hogy a termék átesett tanúsítási eljáráson. A címkék, a tanúsítási eljárások során minősített termékeken kerülnek elhelyezésre. Például a „CE" jelölés az Európai Gazdasági Közösség (EGK) piacán megjelenő termékeken kerül feltüntetésre. A fogyasztók számára azt hivatott jelezni, hogy az EGK-ban forgalmazott termék megfelel az előírt biztonsági, egészségügyi és környezetvédelmi követelményeknek. A „CE" jelölés szabályozása az EU harmonizációs jogszabályainak része, mely felügyeletét az Európai Bizottság Belső Piaci, Ipar-, Vállalkozás- és Kkv-politikai Főigazgatósága a felelős. Az EU termékszabályainak végrehajtására vonatkozó átfogó útmutatás az úgynevezett *Kék Könyv*-ben[16] található. A „CE" címke feltüntetése a gyártó vagy meghatalmazott képviselője kötelezettsége a gyártás végső ellenőrzési fázisában. A „CE" jelölést követnie kell a tanúsított terméket forgalmazó szervezet azonosító számának.[17]



2. ábra: A „CE" jelzés (Conformité Européenne – Európai Megfelelőség)[18]

Folyamattanúsítás alatt a tanúsító szervezet az adott termék vagy szolgáltatás előállításának folyamatát hivatott ellenőrzi. Célja annak egyértelmű bizonyítása, hogy valamely folyamat megfelel a vonatkozó normákkal, szabványokkal, vevői igényekkel, technológiai előírásokkal meghatározott követelményeknek. Biztonsági

---

15 MSZ EN ISO 9000, MSZ EN ISO 19011

16 The 'Blue Guide' on the implementation of EU product rules 2016, Brüsszel, 2016.

17 CE marking, Európai Bizottság Belső Piaci, Ipar-, Vállalkozás- és Kkv-politikai Főigazgatóság, Brüsszel, http://ec.europa.eu/growth/single-market/ce-marking_hu (Letöltés ideje: 2019. 02. 26.)

18 Uo.

szempontból vizsgálat tárgyát képezheti a termelési folyamat lépései során meghatározott elektronikus biztonsági kritériumok megvalósulása.

Rendszertanúsítás során általánosan a tanúsítandó rendszer működését vizsgálják olyan szempontból, hogy az a vonatkozó normáknak megfelelően és a rendszer dokumentációjában leírtak szerint üzemel-e. Ezt az eljárást helyszíni audit során hajtják végre az akkreditált tanúsító szervezet feljogosított szakemberei. Az eredményes vizsgálatot egy adott érvényességi idejű tanúsítványban deklarálják, amelynek hitelességét a kiállító jelzései, aláírása, regisztrációja és azonosítási rendszere igazolja.

Személytanúsítás során egy külső szervezet tanúsítja, hogy az eljárással érintett személy rendelkezik azokkal a szakmai-elméleti ismeretekkel, valamint gyakorlati tapasztalattal, amely feljogosítja a tevékenység végzésére. Az eljárás során vizsgálják az egyén személyi tulajdonságait, képzettségét, gyakorlatát, munkaköri tapasztalatait, továbbá elméleti és gyakorlati vizsga kerül lebonyolításra. A tanúsító szervezet a tanúsítványt egy előre meghatározott időszakra (3-5 évre) adja ki, illetve a meghatározott időintervallumon belül is rendszeresen ellenőrzésre kerül a tanúsítással érintett annak érdekében, hogy meg lehessen bizonyosodni a követelmények folyamatos érvényesüléséről.[19]

2.1. Jelenleg érvényben lévő néhány tanúsítási eljárás

Általános nemzetközi ajánlások:

a. CC ISO/IEC 15408 szabvány

1996-ban a TCSEC,[20] ITSEC,[21] CTCPEC[22] bázisán kiadásra került a Common Criteria[23] (továbbiakban: CC) de facto szabvány. Szádeczky szerint: „*a CC az az informatikai biztonsági termékszabvány, amely ma az informatikai biztonság területén etalonnak tekinthető, a világon egyre szélesebb körben elfogadott és folyamatos fejlesztés alatt áll.*”[24] Az 1.0-ás kiadást az Európai Közösség, az USA és Kanada egyhangúan fogadta el, a 2.0-ás verziója ISO/IEC 15408 jelzettel de jure nemzetközi szabvánnyá vált. Nemzetközi szinten az ISO/IEC 15408 szabvány ad

---

19 DR. KARDOS Károly – DR. JÓSVAI János: Termelő rendszerek minőségbiztosítása, 1. A gyártási folyamat minőségbiztosítása, Széchenyi István Egyetem, 2014. https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0006_termelo_rendszerek_minosegbiztositasa/page72.html (Letöltés ideje: 2019. 02. 17.)

20 Trusted Computer System Evaluation Criteria – Biztonságos Számítógépes Rendszerek Értékelési Kritériumai

21 Information Technology Security Evaluation Criteria – Információtechnológiai Biztonsági Értékelési Kritériumai

22 Canadian Trusted Computer Product Evaluation Criteria – Kanadai Megbízható Számítástechnikai Termékek Minôsítési Követelményrendszere

23 Common Criteria for Information Technology Security Evaluation – Az Információs Technológia Biztonsági Értékelésének Közös Kritériuma

24 SZÁDECZKY Tamás: Információbiztonsági szabványok, egyetemi jegyzet, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, NKE, Budapest, 2014., https://vtkk.uni-nke.hu/document/vtkk-uni-nke-hu/Inform%C3%A1ci%C3%B3biztons%C3%A1gi%20szabv%C3%A1nyok.pdf, p. 16. (Letöltés ideje: 2019. 02. 17.)

iránymutatást az IKT-eszközök tanúsításával kapcsolatban, azonban nemzeti és szervezeti ratifikálása – ajánlás funkciója miatt – nem kötelező jellegű. Az ISO/IEC 15408 a legszélesebb körben elterjedt nemzetközi szabvány, mely kiterjedt nemzetközi hálózattal rendelkezik. A szabvány az IKT-termékek, -rendszerek biztonságának értékeléséhez határoz meg követelményeket, szempontokat és eljárásmódot annak érdekében, hogy megvalósuljon azok bizalmassága, sértetlensége és rendelkezésre állása, mint alapvető elvárás. A szabványban a funkcionális és bizonyossági kritériumok, valamint értékelési bizonyossági szintek mátrixaként határozhatóak meg az alkalmazandó biztonsági követelmények. A követelmények konkretizálása céljából az eszköz fajtájára jellemző védelmi profilok (PP – Protection Profile) alapján biztonsági célkitűzést (ST – Security Target) kell kidolgozni, mely már az eszköztípusra vonatkozó követelményeket tartalmazza. Ez alapján kerül bevizsgálásra maga a termék, a vizsgálat tárgya (TOE – Target of Evaluation).[25] E szabvány által megkövetelt tanúsítási eljárás biztosítja, hogy a termékeket csak független, megfelelő szakmai kompetenciákkal és engedéllyel rendelkező laboratóriumok értékeljék, továbbá meghatározzák, hogy azok milyen mértékben tesznek eleget bizonyos biztonsági követelményeknek, illetve garanciáknak. Garantálja, hogy a tanúsítási folyamat során felhasznált dokumentumokat elkészítsék, melyek meghatározzák, hogy a különböző technológiák tanúsítása során hogyan alkalmazzák a kritériumokat és az értékelési eljárásokat. Garanciát nyújt, hogy a tanúsítandó termékek biztonsági tulajdonságainak értékelése után, az értékelés eredményétől függően eltérő szintű tanúsítvány adható ki. A tanúsítványokat minden a CCRA[26]-t ratifikáló állam elfogadja.[27]

3. ábra: A CCRA egyezmény keretében elismert tanúsítványokon szereplő jelzés[28]

Az ISO tanúsítási eljárás negatívumai közé tartozik, hogy a folyamat hosszú időt vesz igénybe és költséges. Az új egységes uniós tanúsítási keretrendszer ezzel szemben azért lehet előnyös, mert azt tagállami szinten is el kell majd fogadni, így nem lesz szükség egyéb nemzeti tanúsítási eljárások lefolytatására. Egy

---

25 SZÁDECZKY Tamás i. m. p. 16.

26 Common Criteria Recognition Agreement – A Közös Szempontok Szerint Kibocsátott Tanúsítványok Kölcsönös Elismeréséről Szóló Nemzetközi Megállapodás

27 HORVÁTH Gergely Krisztián: Adatbiztonság, Common Criteria (MSZ/ISO 15408:2009), ÁROP–2.2.21 Tudásalapú közszolgálati előmenetel, BGF, Budapest, 2013. https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0003_13_adatbiztonsag/common_criteria_msz_iso_15408_2009__U8mGTKIje2ELLxTm.html (Letöltés ideje: 2019. 02. 17.)

28 International Agreements, Agence nationale de la sécurité des systèmes d'information, https://www.ssi.gouv.fr/en/certification/common-criteria-certification/international-agreements/ (Letöltés ideje: 2019. 02. 18.)

tanúsítvánnyal ki lehet lépni az EU-s IKT-piacra a forgalomba hozni kívánt termékekkel és szolgáltatásokkal. A tanúsítás díját csak egyszer kell megfizetni, továbbá egy sokkal szélesebb piacon valósulhat meg a kereskedelem, így a plusz profit ellensúlyozhatja az eljárási díjakat.

Fontos megjegyezni, hogy a megfogalmazott kritériumok nem alkalmazhatóak egységesen minden technológiára, szektorra, mely az unió szektoriális megközelítéséből fakad.

b. SOG-IS[29] irányelv

Európai szinten jelen lévő egyik fő tanúsítási mechanizmus. Már korábban elkezdődött egy folyamat annak érdekében, hogy Európában kölcsönösen elismerjék a tanúsítványokat, azonban ez csak részben volt sikeres. Erre szolgál például a Vezető Tisztviselők Információs Rendszerek Biztonságával Foglalkozó Munkacsoportján (továbbiakban: SOG-IS) belül elfogadott kölcsönös elismerési megállapodás. A megállapodás a biztonsági tanúsítás terén a legjelentősebb példa az együttműködésre és a kölcsönös elismerésre, azonban magas költségei és korlátozott alkalmazási köre számottevő hiányosságnak számítanak. A legnagyobb hátrány, hogy a SOG-IS csoport csak 9 tagállamot foglal magában, valamint Norvégiát, és csak néhány védelmi profilt fejlesztett a digitális termékekre – például a digitális tachográf-készülékre, a digitális aláírásra és az intelligens kártyákra vonatkozóan –, azonban a belső piac szempontjából a kölcsönös elismerési megállapodás is csak korlátozott hatékonyságú. A résztvevők együtt dolgoznak a közös kritériumokon alapuló védelmi profilok szabványosításának koordinálásán, és ők irányítják az ilyen profilok kidolgozását is.[30]

4. ábra: A SOG-IS egyezmény keretében elismert tanúsítványokon szereplő jelzés[31]

[29] Senior Officials Group on Information Systems Security (https://www.sogis.org/)

[30] Javaslat, AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az Európai Uniós Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály"). COM(2017) 477 final/3 2017/0225 (COD),Európai Bizottság, Brüsszel, 2018. február 22., https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN, p. 36. (Letöltés ideje: 2019. 02. 17.)

[31] International Agreements, Agence nationale de la sécurité des systèmes d'information, https://www.ssi.gouv.fr/en/certification/common-criteria-certification/international-agreements/ (Letöltés ideje: 2019. 02. 18.)

Nemzeti sémák:

a. Franciaország

A biztonsági kritériumok, az értékelési módszerek és eljárások, az ANSSI[32] által meghatározott szabványok alapján történnek, az így kiadott tanúsítványt főleg Franciaországban ismerik el, mivel nincs közös megállapodás azok egységes uniós elfogadására. A szervezet tanúsítási jelentéseket állít ki, melyek meghatározzák az elérni kívánt biztonsági célokat. A jelentések tartalmazzák továbbá azon biztonsági kockázatokat, melyeket a jelentés összeállítói feltárnak és fontosnak tartanak feltüntetni biztonsági okokból. A megrendelők eldönthetik, hogy ezeket a figyelmeztetéseket nyilvánosságra hozzák-e a fogyasztók számára.[33]

b. Németország

A BSI[34] adja ki az IT-Grundschutz Tanusítványt, ami hasonló a franciához. A BSI által alkalmazott szabvány „IT Baseline Protection Manual" néven ismert, mely egy biztonsági szabvány. A hatékonyságát jelzi, hogy az észt informatikai rendszerekben feldolgozott adatokat, olyan háromszintű IT-biztonsági rendszer (ISKE[35]) védi, amelyet a fenti német biztonsági szabvány bázisán, célirányosan az észt közigazgatási szektor kritériumaihoz igazítottak, továbbá melynek alkalmazására minden elektronikus adatbázist és nyilvántartást kezelő önkormányzati és állami szerv köteles.[36]

c. Nagy Britannia

Az NCSC[37] végzi az eljárást, irányító szerve a GCHQ,[38] mely a brit nemzetbiztonsági közösség részét képező intézmény. SIGINT[39] tevékenységet végez, valamint felelős a brit kormány és a fegyveres erők információvédelméért. Személytanúsítási rendszere a Certified Cyber Professional (CCP), mely az elektronikus információbiztonsági szakemberek számára nyújt tanúsítványt. Az eljárással érintett személyek tanúsítása lehetővé teszi, hogy igazolni tudják,

---

[32] Agence nationale de la sécurité des systèmes d'information – Nemzeti Információs Biztonsági Ügynökség (https://www.ssi.gouv.fr/)

[33] ANSSI-CC-2012/76 tanúsítási jelentés, Informatikai Rendszerek Nemzeti Biztonsági Hivatala Párizs, 2012. 201, hiteles.gov.hu/letoltes/140/IDClassic340_cert_report_HU.docx (Letöltés ideje: 2019. 02. 18.)

[34] Bundesamt für Sicherheit in der Informationstechnik – Német Szövetségi Információbiztonsági Hivatal (https://www.bsi.bund.de/DE/DasBSI/dasbsi_node.html)

[35] Infosüsteemide Kolmeastmeline Etalonturbe Süsteem – Három Szintű Információbiztonsági Szabályozási Rendszer.

[36] SÄRAV, Sandra – KERIKMÄE, Tanel – KASPER Ágnes: Az e-polgárság, mint a virtuális migráció eszköze Észtországban, Információs Társadalom, 2016. XVI. évfolyam 2. szám https://informaciostarsadalom.infonia.hu/index.php/inftars/article/view/19, pp. 22-23. (Letöltés ideje: 2019. 02. 18.)

[37] National Cyber Security Centre – Nemzeti Kibervédelmi Központ (https://www.ncsc.gov.uk/)

[38] Government Communications Headquarters – Kormányzati Kommunikációs Központ (https://www.gchq.gov.uk/)

[39] Signal Intelligence – Rádiójel és rádióelektronikai hírszerzés.

rendelkeznek azon jogosultságokkal, ismeretekkel és készségekkel, amelyek szükségesek egy minősített elektronikus információbiztonsági szakember számára.[40]

3. A komplex kiberbiztonsággal és az IKT-termékek tanúsítási eljárásaival kapcsolatos problémák

A tanúsítási eljárások, illetve a komplex kiberbiztonságot érintő problémák alapvetően az IKT-eszközök IoT-ban lévő fokozódó jelenlétéből, az univerzális védelmi stratégia hiányából, valamint a támadások globális jellegéből adódnak. Jelentős gond, hogy a piaci szereplők számára a rendelkezésre álló információk egyenlőtlenül oszlanak meg, melynek gyakori következménye az árukkal szembeni vásárlói bizonytalanság. Vincze János közgazdász szerint ezt a folyamatot a közgazdaságtanban is versenykorlátozó tényezőnek tekintik, melynek csökkentése szükséges a fogyasztói bizalom helyreállítása érdekében. [41] Az IKT-eszközök univerzális felhasználása fokozza jelenlétüket és szerepüket az IoT-ban, így növeli a felületi támadások, incidensek lehetőségét, hiszen a különböző szektorok és iparágak infrastruktúrái kölcsönhatásban vannak egymással. Egy ágazatban jelentkező incidens az univerzitás okán képes eszkalálódni más ágazatoknál is. A fogyasztók egyre több biztonságtechnikai terméket vásárolnak, melyek lassan alapvető fogyasztási cikké válnak. A termékek és szolgáltatások tömeges alkalmazása az információk optimalizálatlan megosztásához vezet, hiszen a vásárlók nem tájékozódnak kellően az eszközök biztonságos kezeléséről, így hozzájárulva az incidensek bekövetkezéséhez, ami az árukkal szembeni vásárlói bizalmatlanságot fogja eredményezni.

3.1. A komplex kiberbiztonsági szektorban jelentkező problémák

Nem jelen publikáció témája, de fontos megemlíteni, hogy a fenti két tényező vezet a teljes kiberbiztonsági szegmenst érintő problémák indikátoraihoz. A problémákat előidéző első ok az, hogy uniós szinten a kiberbiztonsági irányítás szétagolt, mivel nemzeti hatáskörben van a szabályozás. Ez nehézségeket okoz az európai és globális szintű versenyben és növekedésben, ami ahhoz vezet, hogy az európai kiberbiztonsági kkv szektor[42] szabályozását nem európai piaci szereplők, hanem harmadik országból származó vállalatok befolyásolják, ezzel gyengítve az európai piacot, valamint még sebezhetőbbé és technikailag függőbbé téve Európát más államokkal, szövetségesi rendszerekkel szemben. További kockázat a szaktudás kiáramlása a kontinensről, mivel a kiberbiztonsági vállalatok nem tudják optimálisan integrálni az uniós intézmények által kiképzett szakembereket, akik jobban kvalifikált harmadik országban működő vállatoknál vállalnak munkaviszonyt. Egy másik előidéző ok az európai kiberbiztonsági ökoszisztémában jelentkező nem megfelelő szintű párbeszéd és koordináció, melynek eredménye, hogy hiányzik egy a kiberbiztonsági termékek megbízhatóságát és értelmezhetőségét biztosító jól

---

[40] Certified Professional, National Cyber Security Center, https://www.ncsc.gov.uk/scheme/certified-professional (Letöltés ideje: 2019. 02. 18.)

[41] VINCZE János: Miért és mitől védjük a fogyasztókat? - Aszimmetrikus információ és/vagy korlátozott racionalitás, Közgazdasági Szemle, 2010. LVII. évfolyam, Budapest, 2010. p. 728. http://epa.oszk.hu/00000/00017/00173/pdf/01_vincze.pdf (Letöltés ideje: 2019. 02. 20.)

[42] Kis- és középvállalkozói szektor.

funkcionáló, egységes keretrendszer. Ez a továbbiakban korlátokat emel a határokon átnyúló, kollektív kiberbiztonság szavatolása elé. Érezhető, hogy az IKT-termékeket gyártó cégeknél és a felhasználóknál hiány van a megfelelő minőségű szaktudásból, ami hozzájárul a fogyasztói ismeretek hiányához, illetve a termékekkel szembeni bizalmatlanságához. A fenti tényezőknek, a komplex kiberbiztonsági szektorban érezhető közvetett hatása az, hogy a piaci szereplők elmulasztják a növekedési lehetőségeket, melyeket egy dinamikusabban fejlődő és jobb versenyképességi mutatókkal rendelkező kiberbiztonsági ipar megteremthetne.

3.2. Az IKT-termékek tanúsítási eljárásaival kapcsolatos problémák

A tagállami szintű, nem koordinált kezdeményezések növelik a tanúsítási rendszerek széttagoltságát, ami a gazdasági szereplők anyagi ráfordításának megduplázódását, a források pazarlását eredményezi. A tanúsítási eljárások ágazati szegmentálása növeli a széttagoltságot az IKT-termékek piacán, ami alacsonyabb szintű versenyt eredményez az IKT-ágazatban. A szakértelem hiánya nem megfelelő felhasználói tudatosságot eredményez a vásárlók tekintetében, azaz a fogyasztók nem ismerik kellően az általuk vásárolt termékeket, ami az IKT-piac tagoltságával együtt az információk elégtelen megoszlásának növekedéséhez vezet. Mindezek közvetett hatása azoknak a növekedési lehetőségeknek az elmulasztása, melyeket a biztonságos európai IKT-termékek tennének lehetővé. A biztonsági paraméterek feltüntetése nem mindig érik el céljukat, a fogyasztó számára túl bonyolultan írják le az információkat, ezért a vásárló nem kellő biztonsággal fogja használni. Amennyiben megfelelő módon alkalmazzák a címkéket, csökkenthetik a vásárlói bizonytalanságot és legyőzhetik az információk egyenlőtlen megosztását. Megoldás lehet növelni az átláthatóságot, valamint biztosítani az optimális információmegosztást a fogyasztók biztonságtudatosságának fokozása érdekében.

A fentiek alapján megállapítható, hogy a jelenlegi IKT-tanúsítási eljárásokkal kapcsolatban több, igen jelentős probléma fedezhető fel. Példaként megemlíthető, hogy az állampolgárok és vállalatok nem ismerik kellőképpen az általuk vásárolt IKT-termékek és -szolgáltatások biztonsági jellemzőit, továbbá a nemzeti és ágazati tanúsítási rendszerek növekedése a piac széttagoltságához és a nemzetközi növekedés akadályozásához vezet.

3.3. A problémák összefoglalása

- A felhasználók és a vállalatok nem rendelkeznek kellő ismeretekkel az általuk vásárolt IKT-termékek és -szolgáltatások biztonsági tulajdonságaival kapcsolatban, továbbá nincs kellő ismeretük a kibertámadások tekintetében.
- A nemzeti és ágazati tanúsítási rendszerek száma nő, ami a piac széttagoltságát erősíti, így gátat szab az egységes digitális piac kialakulásának.
- A fokozódó kibertámadások okán az uniós intézmények, hivatalok számára okozott nettó veszteségek nem csökkennek, a biztonságra fordítható források nem állnak optimális mértékben rendelkezésre.
- A kiberbiztonsággal kapcsolatos tagállami szemléletek, szakpolitikák eltérőek.

3.4. Elérendő célok

- Kiberbiztonsági kérdésekben a tagállamok közti együttműködés és kooperáció, valamint kollektív fellépés és eljárásrendszer bevezetése, a nemzeti vagy ágazati megoldások helyett, egy egységes kiberbiztonsági szemlélet kialakítása érdekében.
- Egy európai IKT-biztonsági tanúsítási keretrendszer felállítása a biztonsági tanúsítási folyamatok nemzeti és ágazati eltéréseinek kiküszöbölésére egy széleskörű európai kiberbiztonsági piac létrehozása érdekében.
- Az IKT-termékek és -szolgáltatások biztonsági jellemzőinek átláthatóbbá tétele a fogyasztók digitális egységes piacba vetett bizalmának helyreállítása, valamint az információk elégtelen megosztásának felszámolása érdekében.
- A polgárok és vállalatok biztonságtudatosságának növelése a kiberbiztonság területén.

4. Szakpolitikai intézkedések

0. lehetőség** – **nem történik változás

Ebben az esetben a Bizottság által jogalkotási intézkedések nem kerülnének végrehajtásra.

Következmények:

- nem lesz megoldható az információk aránytalan megosztásának kérdése és a jelenlegi tanúsítási folyamatok hatékonyatlansága;
- egyre nehezebb lesz a vásárlóknak tájékozódnia az IKT-termékek és -szolgáltatások biztonsági paramétereiről;
- kicsi a valószínűsége, hogy létrejönne egy megfelelő önszabályozást biztosító jogszabály, így stabilizálódik a fennálló információs rés;
- nagy valószínűséggel növekedni fog a piaci széttagoltság rövid- és középtávon, valamint nőni fog a nemzeti és ágazati tanúsítási eljárások száma,
- a koordináció és az egységes szabályozási rendszer hiánya lehetetlenné teszi a digitális egységes piac létrejöttét.

A fentiek alapján kijelenthető, hogy negatív társadalmi hatása lenne a **0. lehetőségnek**, hiszen a realizálódó többletköltségek a végfelhasználókat (háztartás, vállalati szektor) terhelnék, emiatt a keresleti oldal szereplői nem lesznek képesek a legmegbízhatóbb IKT-termékeket magasabb piaci áron megvásárolni.

1. lehetőség** – **nem jogalkotási aktus** (puha jogi intézkedések)**:

A Bizottság támogatná a tagállamok és a vállalati szektor kezdeményezéseit, például a megfelelő útmutatók és módszerek kidolgozását, továbbá népszerűsítené a SOG-IS közös megegyezés elfogadását. Ennek célja, hogy ösztökélje a biztonsági tanúsítási rendszerek létrehozását, nem kötelező jellegű szakpolitikai eszközökkel,

önkéntes alapon. Ez egy alacsony költségvetésű megoldás lenne, de várhatólag nem lenne megfelelő a piaci széttagoltság kezelésére.

2. lehetőség – ***Uniós jogalkotási aktus*** *(a SOG-IS megállapodás kiterjesztése a tagállamok számára)**:***

Ebben az esetben a Bizottság minden tagállam számára kötelezővé tenné a SOG-IS megállapodás ratifikálását. Ez csak a különböző szabványok SOG-IS által támogatott ajánlásainak alkalmazását tenné lehetővé az eljárások során, mellőzve például az egyéb ágazati, nemzeti módszereket. A Bizottság pénzügyileg támogatná az összehangolt védelmi profilok meghatározását.

3. lehetőség – ***egy egységes uniós kiberbiztonsági tanúsítási keretrendszer kidolgozása***

A javaslat szerint a Bizottság egy európai szintű kiberbiztonsági tanúsítási keretrendszer kidolgozását rendelné el, mely megalkotására felállítana egy, a 28 tagállam kiberbiztonsági ügynökségeinek képviselőiből álló nemzetközi szakértői testületet. A keretrendszer elsődlegesen a már meglévő IKT-biztonsági szabványokon alapulna, mint például a felülvizsgált ISO/IEC 15408 szabvány vagy a SOG-IS megállapodás ajánlásai. Azonban a tagállamoknak lehetősége lenne arra, hogy nemzeti, valamint ágazati eljárásaikat a testület számára benyújtsák, és ha azok bizonyos rendelkezéseit a testület elfogadja, akkor bekerüljenek az egységes IKT-biztonsági tanúsítási keretrendszerbe. Így létrejöhetne egy olyan keretrendszer, mely révén minden tagállam számára elfogadható tanúsítási keretrendszert lehetne kialakítani. Ez a megoldás eléggé rugalmas és kezelhető ahhoz, hogy az elvárásoknak megfeleljen.

5. A támogatott kiberbiztonsági tanúsítási szakpolitikai javaslat

Az összefoglaló jelentésben részletezett szakpolitikai javaslatok közül, az európai jogalkotó szervek a ***3. lehetőség***-et részesítették előnyben.

Ennek köszönhetően nemzetközi konzultáció és koordináció útján jön létre az egységes európai kiberbiztonsági tanúsítási keretrendszer. Az együttműködés véleményem szerint lehetne regionális szintű – azaz az EU tagállamok mellett részt vehetne benne az Egyesült Királyság (a BREXIT után), Svájc, Norvégia, Izland, valamint Liechtenstein is –, hiszen így az uniós piac kibővített változatán folyhatna a biztonságos termékek és szolgáltatások kereskedelme. Természetesen az egységes keretrendszer jelenleg csak uniós szintű szabályozást biztosít, hiszen ez is a célja, azonban később érdemes lehet felülvizsgálni nemzetközi elfogadtatását is. A keretrendszer a meglévő nemzetközi irányelvekre, szabványokra fog alapulni, azonban lehetőség lesz a nemzeti és ágazati tanúsítási rendszereket is figyelembe venni, így érvényesítve a nemzeti, ágazati érdekeket a nemzetközi elvárásokkal összhangban. A nemzetközi koordináció érdekében mandátumának felülvizsgálata utána az ENISA lesz felelős a keretrendszer részeként jóváhagyott tanúsítási rendszerek nyilvántartására, a szabványügyi testületekkel való kapcsolattartásra, valamint a szabványosítást igénylő további IKT területek meghatározására. Továbbá a jogszabály létrehozza az Európai Kiberbiztonsági Tanúsítási Csoportot, mely a

tagállamok nemzeti tanúsítás-felügyeleti hatóságinak delegáltjaiból fog állni. Dr. Bencsik Balázs, a Nemzeti Kibervédelmi Intézet igazgatójának publikációja szerint: „*a csoport fő feladata, hogy tanácsot adjon a bizottságnak a kiberbiztonsági tanúsítási politikát érintő kérdésekben, és együttműködjön az ENISA-val az európai kiberbiztonsági tanúsítási rendszerek tervezetének kidolgozásában.*”[43]

A Bizottság felkérése alapján a keretrendszer kidolgozása az ENISA feladata az Európai Kiberbiztonsági Csoport támogatásával. Fontos kihangsúlyozni, hogy a nemzeti rendszerekkel szemben támasztott kritériumok közé tartozna, hogy rendelkezzenek a kiberbiztonsági követelmények részletes leírásával, az érintett IKT-áruk azonosíthatóságával, legyenek konktért értékelési módszereik és kritériumrendszerük, továbbá deklarálva legyenek a biztonság elérendő szintjei. A jogszabály 3 szintet különböztet meg:

- alap szint: az IKT-termék, -szolgáltatás vagy -folyamat védve van az ismert eredetű, jellegű incidensektől;
- jelentős szint: az IKT-termék, -szolgáltatás vagy -folyamat képes preventíven fellépni a kibertámadásokkal szemben, továbbá képes ellenállni korlátozott mennyiségű erőforrás rendelkezésre állása esetén;
- magas szint: az IKT-termék, -szolgáltatás vagy -folyamat képes preventíven fellépni az kibertámadásokkal szemben, továbbá képes velük szemben ellenállni igen jelentős erőforrás felhasználása mellett is.[44]

A javaslat egyik további főbb célkitűzése, hogy a biztonságosság szempontja már az IKT-termékek és -szolgáltatások fejlesztése, gyártása során érvényre jusson, így biztosítva a *tervezett biztonság elvének*[45] megvalósulását.

A támogatott szakpolitikai javaslatnak köszönhetően meg fog szűnni a tanúsítási rendszerek széttagoltsága, az IKT-piacon realizálódó alacsony szintű verseny, valamint az információk aránytalan megoszlása a piaci szereplők között, így elkezdődhet az európai IKT-termékek és -szolgáltatások piacának növekedése. A teljes kiberbiztonsági piac európai szereplőinek nőhet a piacformáló befolyása, működhet a határokon átnyúló kooperáció. A piac fellendülésének a kiberbiztonsági ellenállóképességek növekedésének okán a kiberbiztonsági szakemberek számára vonzóvá válhat az európai kiberbiztonsági szektor, így magasabb profit realizálódhat az ágazatban. Ezen eredmények hatására az elvárásoknak megfelelően csökkenni fognak a biztonsági incidensekből adódó nettó veszteségek, el fog tűnni az akadály a

---

[43] BENCSIK Balázs: A kiberbiztonsági feladatok kezelése az európai uniós jogalkotás fényében, Belügyi Szemle 2019. LXVII. évfolyam 1. szám, Belügyminisztérium, Budapest, 2019. p. 101.

[44] NEGREIRO, Mar: ENISA and a new cybersecurity act, Briefing EU Legislation in Progress, Európa Parlament Kutatószolgálata, Brüsszel, 2018. p. 14. http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf (Letöltés ideje: 2019. 02. 20.)

[45] „Security by Design” – Lásd: Building an effective response to strengthen Europe’s cyber resilience - The EU Cybersecurity Act proposal, American Chamber of Commerce to the European Union, Brüsszel, 2018. p. 3. https://www.amchameu.eu/system/files/position_papers/amcham_pop_eu_cybersecurity_act_final_1.pdf (Letöltés ideje: 2019. 02. 20.)

digitális egységes piac megteremtése elől, valamint növekedésnek fognak indulni a piaci szereplők.

A tagállamok között egyetértés van abban, hogy a folyamatok koordinálására szükség van a nemzetközi uniós szervezetre, mely megfelelő jogosultságokkal, szakmai tudással és anyagi forrásokkal rendelkezik a jelenlegi és prognosztizált kibertámadások megelőzése, elhárítása érdekében. Közös álláspont alakult ki a kollektív IKT-biztonsági tanúsítási keretrendszer létrehozása érdekében is. A vállalati szektor azon szeplőitől, akik jelenleg is tanúsítási eljárás hatálya alá tartoznak, támogatást élvez a szakpolitikai célkitűzés, mivel így nőhet versenyképességük uniós szinten. A kkv-szektor szintén támogatja az uniós szintű koordinációt, mely képes szavatolni a kiberbiztonsági képességek javítása érdekében hozott intézkedések végrehajtását az ellenálló képesség fokozása érdekében. Az uniós szintű koordinációért felelős szervezet költséghatékony módon történő megreformálása útján az ENISA lesz, mivel így nem kell egy új intézmény felállítására jelentős többletforrást fordítani. Külön tagállami ráfordítást a szervezeti átalakítás szintén nem igényel, mivel ezeket az uniós költségvetés tudja fedezni, tagállami költségek csak a nemzeti tanúsítási hatóságok felállítása és fenntartása során jelentkezhetnének. A kollektív tanúsítási keretrendszer nem járna számottevő többletforrás ráfordításával a kkv-szektor tekintetében sem, sőt a tanúsítási eljárás alá eső piaci szereplők számára megtakarítást is eredményezne, melyek befektetésével hozzájárulhatnak a piaci növekedéshez.

6. Magyarország előnyei a *„kiberbiztonsági jogszabály”*-nak köszönhetően

Az előnyben részesített szakpolitikai javaslat szerint ki fog alakulni egy egységes, nemzetközi irányelveket és nemzeti, ágazati érdekeket figyelembevevő IKT-biztonsági tanúsítási keretrendszer a tagállamok között. Magyarország számára azért lesz előnyös ez a megoldás, mert érvényesíteni tudja nemzeti érdekeit a meglévő tanúsítási rendszerével kapcsolatban abban az esetben, ha az nemzetközi szinten is támogatható. A szakpolitikai intézkedés hatására a magyar IKT-szektor kollektív tanúsítási eljáráson keresztülmenő termékeinek nemzetközi exportja fellendülhet, mivel nem válna szükségessé a célországban elfogadott újabb költséges, időigényes eljárás lefolytatása. Az import tekintetében a külföldi eredetű termékek magyar piacon történő értékesítése is hatékonyabb lenne, mivel ez esetben sem kellene újabb hazai tanúsítási eljárást lefolytatni, így támogatva az áruk és szolgáltatások szabad áramlását, valamint a digitális egységes piac megteremtését.

Az egységes keretrendszer biztosítani fogja továbbá a tájékoztatás összehangolását is, mely során a fogyasztókat a megfelelő módon lehet tájékoztatni a termékek és szolgáltatások biztonsági paramétereiről, így sikerülhet kiküszöbölni az információk nem megfelelő megoszlását a piaci szereplők között, valamint növelni a biztonságtudatosságot, melyek a magyar IKT-piac növekedését fogják eredményezni. A kiberbiztonsági képességek területén is pozitív hatást válthat ki a kollektív tagállami fellépés az incidenskezelés, képzés területén, hiszen a kibertámadások globális eszkalációja okán Magyarország is ki van téve a közvetett és közvetlen támadások okozta negatív következményeknek. Sokkal hatékonyabban lehetne fellépni egy egységes kibertéri ökoszisztéma kialakítása során a támadások hatékonyabb megelőzése, elhárítása érdekében. Ez a folyamat hozzájárulhat az uniós

– köztük a magyarországi – vállalatok növekedéséhez, mely eredményeképpen fokozódhat piaci szerepük, így csökkentve a harmadik országos vállalatok befolyását az uniós piacon, továbbá növelhető lenne a tagállamok kiberbiztonsági ellenálló képessége is.

A fentiek alapján kijelenthető, hogy Magyarország számára az uniós szinten is támogatott szakpolitikai intézkedés gyakorolja a legpozitívabb hatást, mind versenyképesség-javulás, mind a kiberbiztonsági ellenállóképesség fejlődésének tekintetében, költséghatékony módon, a nemzetközi irányelvek, valamint a DSM-stratégiában meghatározott szempontok figyelembevételével, az uniós szinten elfogadott nemzeti érdekek érvényesítésének lehetősége mellett, az Európai Unió kiberbiztonsági tanúsítási keretrendszere terén.

7. Összefoglalás

Az igényeknek megfelelően kialakított stratégiai cél, hogy létrejöjjön az egységes európai IKT-biztonsági tanúsítási keretrendszer, amely megszünteti a tagállami és ágazati eljárások általi széttagoltságot, az elfogadott kiberbiztonsági tanúsítási szakpolitikai javaslat alapján biztosítottá válik. Az új keretrendszer a lehető legharmonikusabban fog illeszkedni a nemzetközi szabványokhoz, bizonyos nemzeti érdekeket is figyelembe véve annak érdekében, hogy csökkenjenek a kereskedelmi akadályok. Az uniós kiberbiztonsági tanúsítási keretrendszer alapvető célja igazolni, hogy a meghatározott kiberbiztonsági kritériumoknak maximálisan megfelelnek az e keretrendszer részeként elfogadott nemzeti tanúsítási eljárások során tanúsított IKT-termékek, -szolgáltatások és -folyamatok. Ez a tevékenység javítja az IKT-termékek és -szolgáltatások biztonságosságát a biztonsági paraméterekről szóló kielégítő tájékoztatást, ezáltal növelve a fogyasztók termékekbe és szolgáltatásokba vetett bizalmát.

Speciális célként került meghatározásra az IKT-rendszerek, -termékek és -szolgáltatások széleskörű lefedettsége, alkalmazhatóságuknak minden tagállamban történő biztosítása, valamint a kiberbiztonsági szektorok biztonsági tanúsításának felülvizsgálata nemzetközi szabványok figyelembevételével, illetve, hogy minden érintett piac és alkalmazó beszerezze ezen tanúsítványokat a termékeihez. Különböző intézkedések kerültek meghatározásra a stratégiai és speciális célok elérése érdekében. Például az ütemtervkészítés, a nemzetközi konzultáció, a hatásvizsgálatok, a tanúsítási eljárások feltérképezése, az intézményrendszer bevonása a szabályozási eljárásba, a szektor-specifikus kérdések vizsgálata, az egységes tanúsítási keretrendszer és a nemzeti rendszerek kidolgozása, a kiberbiztonsági testület létrehozása, valamint ágazati szintű munkacsoportok felállítása. Ezen intézkedések hozzájárulnak a kiberbiztonság egységes szabályozásához, az információk egyenlőtlen megoszlásának csökkentéséhez, a felhasználók kiberbiztonsági ismereteinek, biztonságtudatosságnak növeléséhez, továbbá az IKT tanúsítási és a kiberbiztonsági piac széttagoltságának felszámolásához. Ezen eredmények várható hatása, az az optimális állapot, mikor csökkennek a kibertámadások okozta nettó veszteségek, javul az IKT-termékek, szolgáltatások és az IoT-alkalmazások kereslete a fogyasztói bizalom visszanyerése okán, így stabilizálódik és növekedésnek indul a digitális egységes piac.

Felhasznált irodalom:

- A tanúsítás folyamata, Eurpoean CERT, http://www.european-cert.hu/ (Letöltés ideje: 2019. 02. 16.)
- Agence nationale de la sécurité des systèmes d'information – ANNSI https://www.ssi.gouv.fr/ (Felhasználás időpontja: 2018. 07. 23.)
- ANSSI-CC-2012/76 tanúsítási jelentés, Informatikai Rendszerek Nemzeti Biztonsági Hivatala, Párizs, 2012. 201,hiteles.gov.hu/letoltes/140/IDClassic340_cert_report_HU.docx (Letöltés ideje: 2019. 02. 18.)
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union - Európai Parlament és Tanács, Brüsszel, 2016. július 6. https://eur-lex.europa.eu/legalcontent/HU/TXT/HTML/?uri=CELEX:32016L1148&from=EN (Letöltés ideje: 2019. 02. 14.)
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - Európai Parlament és Tanács, Brüsszel, 2016. április 27., https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Letöltés ideje: 2019. 02. 14.)
- BENCSIK Balázs: A kiberbiztonsági feladatok kezelése az európai uniós jogalkotás fényében, Belügyi Szemle 2019. LXVII. évfolyam 1. szám, Belügyminisztérium, Budapest, 2019. pp. 93-107. ISBN 1789-4689
- Building an effective response to strengthen Europe's cyber resilience - The EU Cybersecurity Act proposal, American Chamber of Commerce to the European Union, Brüsszel, 2018. https://www.amchameu.eu/system/files/position_papers/amcham_pop_eu_cybersecurity_act_final_1.pdf (Letöltés ideje: 2019. 02. 20.)
- Bundesamt für Sicherheit in der Informationstechnik – BSI https://www.bsi.bund.de/DE/DasBSI/dasbsi_node.html (Letöltés ideje: 2018. 07. 23.)
- CE marking, Európai Bizottság Belső Piaci, Ipar-, Vállalkozás- és Kkv-politikai Főigazgatóság, Brüsszel, http://ec.europa.eu/growth/single-market/ce-marking_hu (Letöltés ideje: 2019. 02. 26.)

- Certified Professional, National Cyber Security Center, https://www.ncsc.gov.uk/scheme/certified-professional (Letöltés ideje: 2019. 02. 18.)
- COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). SWD/2017/0500 final 2017/0225 (COD), Európai Bizottság, Brüsszel, 2017. szeptember 13., https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52017SC0500 (Letöltés ideje: 2018. 07. 22.)
- DR. GREGÁSZ Tibor: A minőségirányítás alapjai Szabványos minőségmenedzsment rendszerek működési elvei, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, NKE, Budapest, 2014, pp. 42-46., https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/a-minosegiranyitas-alapjai.original.pdf (Letöltés ideje: 2018. 08. 10.)
- DR. KARDOS Károly – DR. JÓSVAI János: Termelő rendszerek minőségbiztosítása, 1. A gyártási folyamat minőségbiztosítása, Széchenyi István Egyetem, 2014. https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0006_termelo_rendszerek_minosegbiztositasa/page72.html (Letöltés ideje: 2019. 02. 17.)
- EU negotiators agree on strengthening Europe's cybersecurity, Cybersecurtiy Act, Európai Bizottság, Brüsszel, 2018. december 11. https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en (Letöltés ideje: 2019. 02. 17.)
- Government Communications Headquarters – GCHQ https://www.gchq.gov.uk/(Letöltés ideje: 2019. 02. 18.)
- HORVÁTH Gergely Krisztián: Adatbiztonság, Common Criteria (MSZ / ISO 15408:2009), ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, BGF, Budapest, 2013. https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0003_13_adatbiztonsag/common_criteria_msz_iso_15408_2009__U8mGTKIje2ELLxTm.html (Letöltés ideje: 2019. 02. 17.)
- International Agreements, Agence nationale de la sécurité des systèmes d'information, https://www.ssi.gouv.fr/en/certification/common-criteria-certification/international-agreements/ (Letöltés ideje: 2019. 02. 18.)
- Javaslat, AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az Európai Uniós Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”). COM(2017) 477 final/3 2017/0225 (COD), Európai Bizottság, Brüsszel, 2018. február 22., https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN (Letöltés ideje: 2019. 02. 17.)

- National Cyber Security Centre – NCSC, https://www.ncsc.gov.uk/ (Felhasználás időpontja: 2018. 07. 24.)
- NEGREIRO, Mar: ENISA and a new cybersecurity act, Briefing EU Legislation in Progress, Európa Parlament Kutatószolgálata, Brüsszel, 2018. http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf (Letöltés ideje: 2019. 02. 20.)
- SÄRAV, Sandra – KERIKMÄE, Tanel – KASPER Ágnes: Az e-polgárság, mint a virtuális migráció eszköze Észtországban, Információs Társadalom, 2016. XVI. évfolyam 2. szám https://informaciostarsadalom.infonia.hu/index.php/inftars/article/view/19, ISSN1587 8694. (Letöltés ideje: 2019. 02. 18.)
- Senior Officials Group on Information Systems Security – SOG-IS, https://www.sogis.org/ (Felhasználás időpontja: 2018. 07. 23.)
- SZÁDECZKY Tamás: Információbiztonsági szabványok, egyetemi jegyzet, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, NKE, Budapest, 2014. p. 16. https://vtkk.uni-nke.hu/document/vtkk-uni-nke-hu/Inform%C3%A1ci%C3%B3biztons%C3%A1gi%20szabv%C3%A1nyok.pdf (Letöltés ideje: 2019. 02. 17.)
- SZŐKE Gergely László: Az önszabályozás, audit és tanúsítás lehetőségei és korlátai az adatvédelem területén, Infokommunikáció és jog, 2014. XI. évfolyam 1. szám, HVG-Orac Lap és Könyvkiadó Kft., Budapest, 2014. p. 14-20., https://infojog.hu/wp-content/uploads/pdf/201457_SzokeGergelyLaszlo.pdf, ISSN 1786-0776 (Letöltés ideje: 2019. 02. 16.)
- VINCZE János: Miért és mitől védjük a fogyasztókat? - Aszimmetrikus információ és/vagy korlátozott racionalitás, Közgazdasági Szemle, 2010. LVII. évfolyam, Budapest, 2010. p. 725–75 ISBN 978-963-89769-2-52, http://epa.oszk.hu/00000/00017/00173/pdf/01_vincze.pdf (Letöltés ideje: 2019. 02. 20.)

DR. KASSAI KÁROLY

KIBERTÉR – AKTUÁLIS VÁLTOZÁSOK

Bevezetés

Logikus feladatszervezés esetén – kiemelten kormányzati, nagyvállalati környezetben – kritikus fontosságú a feladatok hierarchiában történő szervezése, beleértve a különböző szintek szerinti felelősségek, hatáskörök és tevékenységek összehangolását. Amikor nemzeti vagy ágazati szintű kommunikációs képességek biztonságos használatáról, igénybevételéről van szó, *az információbiztonsági kérdések, vagy más nézőpont szerint a kiberbiztonsági (vagy kibervédelmi) kérdések megkerülhetetlenek.*

Az utolsó néhány évben olyan változások következtek be a nemzetközi színtéren, ami az EU-s, NATO-követelmények vonalán nemzeti szintű reagálásokat követel.

A nemzetközi színterű változások üzenete egyszerű: rengeteg példán keresztül érzékelhető, hogy *a kibertérben tapasztalható fenyegetések, a szolgáltatásokban, termékekben feltárt sérülékenységek a korábbihoz képest nagyságrendekkel emelik a veszélyességi szintet, civil és katonai értelmezés szerint egyaránt.*

Ennek alapján az elmúlt hónapokban a magyar kibervédelmi keretrendszer-szabályozás és felelősségek tekintetében több ponton módosult, így a katonai kibertér műveleti képességekre vonatkozó követelmények, illetve a képességfejlesztés szempontjából is fontos a nemzeti és katonai stratégiai szinten bekövetkezett változások megértése.

A publikáció az EU-s, NATO és nemzeti stratégiai szintű változások lényegi elemeit mutatja be, hogy érzékelhető legyen ennek az új szakterületnek, szemléletmódnak a változása, fejlődése. A „hálózatbiztonsági", „elektronikus információvédelmi" vagy „kibervédelmi" megfogalmazások esetenként egymást átfedik, tartalmi értelmezésük keveredik, így a források megfogalmazásait figyelmesen kell követni, illetve támogatni kell minden terminológiai továbblépést a jelenlegi helyzet javítása érdekében – de ezt nem ennek az írásnak a feladata.

Fontos annak megfogalmazása, hogy a változások nyomon követéséhez, pontos megértéséhez *a vezetők, elektronikus információs rendszerek biztonságáért felelős személyek, informatikai vagy egyéb üzemeltető állomány számára nélkülözhetetlen a szabályozók adott beosztáshoz köthető szintű ismerete.*

EU-s hálózatbiztonsági irányelv megjelenése - 2016

Nemzeti szinten kiemelt fontosságú esemény, hogy a 2013-as Nemzeti Kiberbiztonsági Stratégia mellett új stratégiai dokumentum jelent meg: Magyarország hálózati és információs rendszerek biztonságára vonatkozó

Stratégiája. A dokumentum a 2016-ban megjelent EU-s követelmény – a hálózati és információs rendszerek biztonságáról szóló irányelv („NIS Directive")[1] adoptálása. Lényegi elemei a következők:[2]

- A nemzeteknek *„hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát" kell elfogadni,* lényegi elemeinél az Irányelv követelményeit követve.
- A delegált tagállamok képviselőiből *együttműködési csoportot kell kialakítani* (információcsere, bizalomerősítés és stratégiai együttműködés), ami a nemzeti egyedüli kapcsolattartó pontokon keresztül valósul meg.
- Az együttműködés technikai szintjének erősítése érdekében számítógép-biztonsági eseményekre reagáló csoportok hálózatát (CSIRT)[3] kell kialakítani és fenntartani.
- *Ki kell alakítani az „alapvető szolgáltatások"* (essential services) kategóriát a kritikus infrastruktúra védelem (hazánkban: létfontosságú infrastruktúra védelem) területén, a társadalmilag kritikus fontosságú szolgáltatások üzemeltetőinek kiemelt figyelemmel történő kezelése érdekében (5. cikk). A „jelentős zavar" (significant disruptive effect) meghatározáshoz tartozó elemek segítik a besorolásban az alkalmazó szervezeteket.
- *Az incidensek bejelentési kötelezettségének kiterjesztése az alapvető szolgáltatásokat nyújtók és a digitális szolgáltatók körére* (hazánkban ez a kötelezettség korábban jogszabályban nem szerepelt).

EU-s ajánlás a nagyszabású kiberbiztonsági eseményekkel kapcsolatban - 2017

Az Európai Bizottság 2017-ben *ajánlást adott ki a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról*[4] annak érdekében, hogy a nemzeti erőforrásokat meghaladó, vagy nemzetek közötti koordinálást igénylő reagálások kellően hatékonyak legyenek.

A dokumentum azonosítja, hogy egy kiberbiztonsági esemény akkor tekinthető uniós-szintű válsághelyzetnek, ha:

- *az adott tagállam azt már nem tudja kezelni*, vagy
- *két vagy több tagállamot é*rint és olyan hatásokat vált ki, amit uniós szinten kell kezelni.[5]

---

1 AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC.

2 Uo. sorrendben: 7, 10, 12, 5, és 14. cikk.

3 Computer Security Incindent Response Team.

4 A BIZOTTSÁG AJÁNLÁSA (2017. 09. 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról, C(2017) 6100 final, Brüsszel, 2017. 09. 13. (Angol megfogalmazás szerint: „…Large Scale Cybersecurity Incinents and Crisis".)

5 Uo. p. 2. A folyamatos fenyegetések és a kiberbiztonsági események miatt a

Az Ajánlás feladatainak nagybani összefoglalása:[6]

- *Kiberbiztonsági válságreagálási keretet* kell kidolgozni (beleértve az Ajánlás melléklete szerinti alapelveknek, célkitűzéseknek és módszertannak megfelelő együttműködést) – mely feladat EU-szinten és tagállami szinten is jelentkezik.
- *Technikai, operatív és stratégiai-politikai szinten azonosítani kell az érintett szereplőket*, az EU-s szervezetekkel történő együttműködést meg kell szervezni. Eljárásokat kell kialakítani a keretrendszeren belüli együttműködés érdekében (súlypont az információcserén és a reagálás összehangoláson van). Tapasztalatszerzési és feldolgozási rendet kell alakítani.
- A kiberbiztonsági válságreagálási keretrendszeren belüli reagálás kidolgozásakor *az EU-s együttműködést be kell dolgozni a nemzeti válságkezelési eljárásokba*.
- A tagállamoknak, EU-s szervezeteknek együtt kell működnie az egységes taxonómiájú kibertérben történt technikai okokat, hatásokat leíró helyzetjelentések kialakítása érdekében.
- Az EU-s és nemzeti szinten értelmezett keretrendszer eljárásait a nemzeti-regionális és EU-s *kibervédelmi gyakorlatok alapján folyamatosan felül kell vizsgálni*, melynek során a Cyber Europe kibervédelmi gyakorlat tapasztalatait súlyozottan kell kezelni.
- *Rendszeresen gyakorolni kell* a nemzeti és EU-s szintű „nagyhatású kiberbiztonsági eseményekre" való reagálást. .

Az Ajánlás mellékletében szereplő alapelvek *stratégiai-politikai, operatív és technikai szintű EU-s reagálási szinteket alakít ki*, így a nemzeti együttműködési rendszert ehhez illesztve célszerű kialakítani. Az említett szinteken végzendő tevékenységek az *összehangolt reagálás*, a *közös helyzetismeret* és a *tájékoztatások*. Az Ajánlás szerint kifejezetten a reagálási fázisra kell összpontosítani.

A kibertéri hatások mellett *figyelembe kell venni az egyéb fizikai hatásokat, más területű válságkezelési feladatokat* is (ágazatokon belüli, ágazatok közötti hatásmechanizmusok figyelembe vétele).

Javaslat az EU Parlament és a Tanács felé – 2017

Az előzőekben vázolt, a kibertérben bekövetkező nagyhatású negatív incidensek ellensúlyozása érdekében az EU Parlament és a Tanács felé történő javaslat Kiberbiztonsági Vészhelyzet-elhárítási Alap (Cybersecurity Emergency Response Fund) felállítását tartja célszerűnek, példaként követve az általános válságkezelési eljárást, ami segíti a legfontosabb első lépések megtételét (eszközcsere finanszírozása, egyéb válaszlépés anyagi támogatása).[7]

---

tagállamoknak 2018 végéig kell cselekedniük az ajánlás alapján.

6 Uo. pp. 7-8.

7 KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Ellenállóképesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése, Brüsszel, 2017.9.13. JOIN(2017) 450 final, p. 2., 4.

EU Kibervédelmi Politikai Keretrendszer (2018)

Az EU Kibervédelmi Politikai Keretrendszer 2018 (Cyber Defence Policy Framework) dokumentum a korábbi, 2014-es Keretrendszer felülvizsgálata.[8]

A Keretrendszer jellegzetessége, hogy a NATO 2016-os döntésével összhangban kijelenti, hogy a kibertér a műveletek ötödik területe a földi, tengeri légi, és világűr tartomány mellett.[9] A védelmi szektorra specializált, Tanács által kiadott, nyilvánosan kevésbé hivatkozott dokumentum hat területet azonosít prioritásként (területenként EU szervezetek és tagállamok feladatait, vagy önkéntes vállalási lehetőségeit) részletezve:

- *A tagállamok kibervédelmi fejlesztéseinek támogatása.* A kibervédelmi képességfejlesztéseknek és technológiáknak le kell fednie a doktrína, vezetés és irányítás, szervezet, tréning, ipar, technológia, infrastruktúra, logisztika és interoperabilitás területeket. A missziók és műveletek követelményei szerint szükség van az infrastruktúrák sérülékenységeinek folyamatos vizsgálatára, a védelem hatékonyságának közel valós idejű megismerésére. Kulcselemek a tagállamok számára:
  - közös „Pooling and Sharing" projektekben való részvétel, a tapasztalatok alapján követelmények, minimum védelmi rendszabályok szabványosítása, önkéntes alapon a PESCO-n[10] belüli együttműködés növelése, a katonai CERT kooperáció erősítése (megelőzés és incidenskezelés);
  - kibervédelmi tréning képességfejlesztés az EU harccsoport vizsgáztatás (certification) érdekében.
- *Az EU szervezetek híradó-informatikai rendszerei védelmének kiterjesztése.* (Kifejezetten EU szervezeti feladat, tagállami szinten nem értelmezhető.)
- *A civil – katonai együttműködés erősítése.* A folyamatos technológiai fejlődés miatt fejleszteni kell a biztonsági megoldásokat. A hasonló területű civil-katonai technológiai fejlesztések esetében erősíteni kell az együttműködést (speciális katonai területeken erre nincs lehetőség). A civil kiberbiztonság erősítése jelentős faktor, ami támogatja a hálózatok ellenálló képességét (resilience). Az EU-s szabályok alkalmazása (NIS irányelvek, EU-s stratégiai szintű összehangolások, incidenskezelési technikai együttműködések a katonai és civil eseménykezelő központok (CERT-ek) között) mind védelmi képességet erősítő tényezők. Kulcselem a tagállamok számára: EU szinten a katonai és civil eseménykezelő szervezetek együttműködésének erősítése.
- *Kutatás és fejlesztés.* A technikai képességek fejlesztése Európában a fenyegetések és sérülékenységek csökkentése szempontjából alapvető fontosságú. A rejtjelző technológiák, a beágyazott rendszerek biztonsági megoldásai (embedded systems), a károskód detektálás, a szimulációs és vizualizációs technológiák, a hálózatok védelmi kérdései, az azonosítási és hitelesítési technológiák azok a területek, melyekkel foglalkozni kell. Emellett erősíteni kell az európai kis- és középvállalatok (KKV) beszállítói lánc biztonságát (supply chain security).

---

8 EU Cyber Defence Policy Framework (2018 update) Brussels, 19 November 2018 (OR. en) 14413/18.

9 Uo. p. 2. Érdekesség, hogy a NATO ennél a megfogalmazás a „világűr"-t nem említi, de ennek ellenére NATO által elfogadott az „5. domain" megfogalmazás.

10 Permanent Structured Cooperation – Állandó Védelmi Kezdeményezés, melynek hazánk is alapító tagja.

– *Az oktatási, képzési és tréninglehetőségek fejlesztése.* A kibervédelmi tréninglehetőségeket fejleszteni kell a kibertér-fenyegetésekre történő felkészülés, a közös kibervédelmi kultúra EU-szintű fejlesztése érdekében, ami egyben a missziók és műveletek védelmét is támogatja. Az oktatási és tréninglehetőségek EU-szintű megosztása is kulcsfontosságú. Fejleszteni kell kibervédelmi gyakorlatokat a civil és katonai szereplők számára, ami egyben eszközként szolgál a kibervédelem megértéséhez. A közös tevékenység erősíti a nemzeti erők felkészültségét a nemzetközi környezetben történő feladatvégrehajtásra, növelik a megbízhatóságot, támogatják az interoperabilitást.
– *A nemzetközi partnerek közötti együttműködés erősítése.* A nemzetközi együttműködés keretein belül biztosítani kell a dialógust a nemzetközi partnerek között (pl. NATO, ENSZ, Európai Biztonsági és Együttműködési Szervezet[11], és egyéb nemzetközi szervezetek), segíteni kell a stratégiai keretrendszer fejlődését a kibertérben történő konfliktusmegelőzés, együttműködés és stabilitás érdekében.

Új nemzeti stratégia

Az EU-s követelmény és a saját nemzeti feladatok (Nemzeti Infokommunikációs Stratégia áttekintése, Digitális Jólét Program) végrehajtása érdekében kormányhatározat rendelte el a 2013-as Nemzeti Kiberbiztonsági Stratégia felülvizsgálatát, illetve a feladatokat és felelősöket tartalmazó intézkedési terv elkészítését.[12]

A Kormányhatározat melléklete elrendelte a már létező Kormányzati Eseménykezelő Központ (GovCERT) mellett a 2013. évi L. törvény kiterjesztési lehetőségének vizsgálatával egy nemzeti kiberbiztonsági eseménykezelő központ kialakítását 2018. 12. 31-ig.[13]

A Stratégia felülvizsgálatának végrehajtása eredményeképpen – *annak fennmaradása mellett* – megszületett a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája, melyet Kormányhatározat fogadott el. Ezzel egyidejűleg a Kormányhatározat a korábbi feladatszabással összhangban elrendelte a kialakított 56 feladat intézkedési terv formájában történő kidolgozását 2019. 03.31-ig.[14]

---

[11] Organization for Security and Co-operation in Europe – OSCE.

[12] 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről, 18. pont.

[13] 1. melléklet az 1456/2017. (VII. 19.) Korm. határozathoz (A Digitális Jólét Program 2.0 2017-2018. évi Munkaterve), 14. b) pont.

[14] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról, 1-2. pont.

A Stratégia[15] elemzése meghaladja a cikk lehetőségeit. A honvédelmi szempontból fontos elemei a következők:

- Az előzmények összefoglalásánál megtörténik a 2013-as stratégia lényegi elemeinek bemutatása, illetve a kapcsolódási pontok azonosítása (Alaptörvény, NATO politikai szintű követelmények, EU-s szakterületi stratégia).
- A Stratégia a hasonló típusú dokumentumok felépítésének logikája szerint összefoglaló jelleggel *megállapítja a kibertér-fenyegetések növekvő tendenciáját, a támadási kísérletek bonyolultságának, veszélyességének növekedését*.
- Megtörténik az eddigi stratégiai irányítási keretrendszer áttekintése (Nemzeti Kiberbiztonsági Koordinációs Tanács, Kiberkoordinátor, Kiberbiztonsági Fórum és Munkacsoportok). A nemzeti szintű felügyelet a Nemzetbiztonsági Szakszolgálat keretén belül működő Kormányzati Eseménykezelő Központot és Nemzeti Elektronikus Információbiztonsági Hatóságot (NEIH) magába foglaló Nemzeti Kibervédelmi Intézetnél (NKI) jelentkeznek, a honvédelmi és polgári nemzetbiztonsági szolgálat kivételével. Ez a két ágazat az eseménykezelő és hatósági felügyeleti feladatokat önállóan látja el. *Az NKI látja el az EU felé a kapcsolattartási funkciót.* A hírközlési szolgáltatók eseménykezelését külön szervezet látja el (HunCERT). *Az oktatási és kutatási tevékenységek összehangolását a Nemzeti Közszolgálati Egyetem, Kibervédelmi Akadémia végzi.*
- A Stratégia által meghatározott feladatok a következő részterületekre tagozódnak:
  - a digitális környezet iránti bizalom erősítése (az együttműködés és tudatosság erősítése, a szakmai irányítás fejlesztése);
  - digitális infrastruktúra-védelem (fejlesztések minőségi menedzsmentje, központi szolgáltatások biztonságának erősítése, nemzetközi együttműködés és létfontosságú infrastruktúra-védelem);
  - a gazdasági szereplők támogatása (innováció, támogatás és koordináció).

A Stratégia a korábbi hasonló szintű szabályozási elemekhez képest új elemmel járul hozzá a védelmi rendszabályokhoz azzal, hogy az általánosan megfogalmazott követelmények érvényesülése érdekében *konkrét nemzeti szintű feladatokat határoz meg*, megalapozza és meghatározza a nemzeti intézkedési terv kialakítását – más nemzetek megoldásaihoz hasonlóan.

A tanulmány írásának idején az Intézkedési Terv feladatai publikusan még nem megismerhetők, de szakmai szempontból egyértelműen kijelenthető, hogy *az előzmények nélküli megoldás fontos lépést jelent a magyar közigazgatásban.* Remélhető a tapasztalatok feldolgozásával a magyar stratégiai irányítási rendszer (SIR) szellemiségével összhangban lévő szabályozási eszköz rendszerbe állítása a kibervédelem, elektronikus információvédelem területén is.

[15] Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája (2018); https://hirlevel.egov.hu/2019/01/13/magyarorszag-halozati-es-informacios-rendszerek-biztonsagara-vonatkozo-strategiaja/; pp. 4-8., 9-10.

A nemzeti stratégia-szint „alatt" a jogszabályok részletes ismertetése helyett szintén csak a lényegi elemek kiemelésére van lehetőség. A legfontosabb változások a következők:

Információbiztonsági törvény - 2013. évi L. törvény (Ibtv.)

Január elsejétől módosítások, új elemek jelentek meg[16] az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben:[17]

- Az értelmező rendelkezésekben megjelent az EU-s követelmények szerinti „*alapvető szolgáltatásokat nyújtó szolgáltató"* kategória, a létfontosságú rendszerek üzemeltetői körének további specializálása érdekében.
- Új elemként törvényi szinten megjelent „*honvédelmi célú elektronikus információs rendszer"* fogalom, ami eddig csak végrehajtási rendeletben szerepelt. A meghatározás rávilágít, hogy *a honvédelmi szervezetek vezetéséhez és irányításához, működéséhez, valamint a külső kapcsolattartáshoz szükséges adatok kezeléséhez zártcélú rendszerek mellett nyílt rendszerek szolgáltatásait is igénybe kell venni, mely esetekben szintén érvényesíteni kell a honvédelmi érdekek fokozott védelmét*.
- A hatóság – amennyiben a jogszabályokban az elektronikus információs rendszerekre vonatkozó biztonsági követelményeket, eljárásokat a költségvetési szerv nem teljesíti – bírságot szabhat ki (a bírság mértéke a végrehajtási rendelet mellékletében részletesen meghatározott).
- *A hatóság végleges határozata az ügyfélen kívül csak külön jogszabályban meghatározott egyedi esetekben ismerhető meg*. Ennek megfelelően *a honvédelmi szervezetek vezetőinek, a parancsnokoknak és az elektronikus információs rendszer biztonságáért felelős személyeknek pontosan kell érteniük a hivatalos okmányok kezelésével kapcsolatos lehetőségeket.*
- A törvény a feladatokat határoz meg *a korai figyelmeztetés* rendjének kialakítása érdekében. Ez azt jelenti, hogy az adott elektronikus információs rendszerek védelmét biztosító saját védelmi mechanizmusok és eljárások kötelező jelleggel kiegészülnek más forrásból érkező információkkal. *A honvédelmi célú elektronikus információs rendszerre vonatkozóan az általános követelmények alapján az ágazatspecifikus szabályokat ki kell dolgozni.*

Hatósági felügyeleti feladatok - 187/2015. (VII. 13.) Korm. rendelet

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságokra vonatkozó jogszabály[18] kisebb, főleg technikainak mondható változásai

---

16 A változások részletesen az egyes belügyi tárgyú és más kapcsolódó törvények módosításáról szóló 2018. évi CXXI. törvény 111 – 119. §-ban olvashatók.

17 Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 1. § (1); 16. § (3) d); 22. § (5); 24. § (1) m) pontok.

18 Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságokra, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet.

a honvédelmi vagy katonai nemzetbiztonsági szempontú kötelezettségeket, feladatokat jelentősen nem érintik.

Új elemként azonosítható az eljáró hatóságok függetlenségére vonatkozó megfogalmazás:

„A hatóság közigazgatási hatósági jogkörében eljárva kizárólag a jogszabályoknak van alávetve, hatósági eljárása során és hatósági döntéseinek tartalmával összefüggésben – a feladat elvégzésére vagy a mulasztás pótlására irányuló utasítás kivételével – nem utasítható."[19]

A jogszabály a Jogkövetkezmények részben tartalmazza az Ibtv. változásnál már bemutatott információkat a kiszabható bírsággal kapcsolatban.

A honvédelmi célú elektronikus információs rendszerek biztonságával kapcsolatos kihívás továbbra is a *szervezeti szint és a rendszerek biztonsági osztályba sorolása* – rendszerspecifikus kockázatelemzésre alapozottan –, az *adott biztonsági szint szerinti védelmi rendszabályok alkalmazása*. Adminisztratív feladatként jelentkezik a hatóság felé[20] szükséges bejelentési kötelezettség alá eső adatok pontosítása, az elektronikus rendszerek biztonságáért felelős (és az eseménykezelési eljáráshoz tartozóan az események kivizsgálásáért felelős) személy azonosítása, képzettségének biztosítása. Ebbe a körbe tartozik a más jogszabályban megváltozott hatósági eljárásrend azon feladata, hogy *a végrehajtott ellenőrzések után a visszaellenőrzés már nem opcionális, hanem kötelezően végrehajtandó elem*.

A fejlesztések során *még a tervezési időszakban véleményezésre meg kell küldeni a rendszerekre vonatkozó elgondolást*, ami alapvető eszköz a később kiderülő hiányzó védelmi rendszabályok, vagy egyéb biztonsági problémák elkerülése érdekében. A honvédelmi szervezetek jelentős része az utóbbi két évben a hatósági ellenőrzési és egyéb felügyeleti feladatokon keresztül gyakorolta a hatósági kapcsolattartást. Jó tapasztalatai vannak az egyedi esetekben szükséges tanácsadásnak is, ami jelzi, hogy az érintett szervezeteknél már elmúlt az „újdonságtól való idegenkedés".

Eseménykezelés - 271/2018. (XII. 20.) Korm. rendelet

A jogszabály az azonos című, 2015-ben kiadott jogszabály újabb kiadása. Lényegi változásai a következők:[21]

– A már említettek szerinti EU-s követelmények átvezetése a magyar jogszabályokban (kiemelten az alapvető szolgáltatást nyújtó szolgáltató, a CSIRT-ek hálózata, illetve a nemzeti kapcsolatttartási feladat).

---

[19] Uo. 2. §. (2) pont. Ugyanez a szabályozási elem jelenik meg a később ismertetett elektronikus minősített adatkezelés szabályozás változásánál (lásd: 161/2010. (V. 6.) Korm. rendelet résznél).

[20] A honvédelmi ágazatnál a hatósági funkciót a Katonai Nemzetbiztonsági Szolgálat főigazgatója látja el.

[21] 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat szabályairól, 1. §. 2, 8) pont; 2. §; 13. §; 3. § c-d) pont; 24. § (1) c-d) pont, és 27. §.

- Az Ibtv. szerinti (központi) eseménykezelő központ feladatellátása a korábbi jogszabály „Kormányzati Eseménykezelő Központ" megfogalmazás helyett a „Nemzetbiztonsági Szakszolgálat által" (megnevezése a jogszabályban: Központ) történik. A Központ látja el az EU követelmények szerinti kapcsolattartó és CSIRT hálózat képviselő szerepet is. *Az eseménykezelő rendszerben továbbra is fennmarad korábbi ágazati eseménykezelési rend, így a honvédelmi szakfeladatok változatlanok.*
- A jogszabályban meghatározott szervezetek számára kötelező az elektronikus biztonsági események jelentése a Központ felé, de *megjelent az önkéntes bejelentési lehetőség a létfontosságú infrastruktúra ágazati szereplők számára* (az alapvető szolgáltatásokat nyújtó szolgáltatói körön kívüli szereplők). Az önkéntes bejelentőre olyan új kötelezettség nem róható a biztonsági esemény kapcsán, mellyel korábban nem rendelkezett.
- A Központ hatásköre bővült, mert az EU vagy nemzeti létfontosságú infrastruktúra-üzemeltetők (honvédelmi rendszerek kivételével), a központosított informatikai és elektronikus hírközlési szolgáltatók is bekerültek az ügyfélkörbe.

Az eseménykezelő központok hatáskörébe tartozó *sérülékenységvizsgálati kör bővült, megjelent az automatizált vizsgálat és a pszichológiai manipuláció*. Új elem, hogy *az eseménykezelő központok saját hatáskörben is indíthatnak sérülékenység vizsgálatokat*.

Az üzemeltető szervezeteknek a webes szolgáltatások, weboldalak és web-szerverek technikai adatait be kell jelenteniük az illetékes eseménykezelő központnak, ami honvédelmi szervezetek esetében is végrehajtandó feladatot jelent. A bejelentett adatokban történő változást három napon belül kell bejelenteni. Az eseménykezelő központ a bejelentő üzemeltető szervezetet tájékoztatja a technikai vizsgálatot végző egyedi technikai azonosító adatokról, melyet az érintett szervezet nem tilthat ki a szolgáltatás elérésből.

Létfontosságú infrastruktúra védelem

A honvédelmi létfontosságú rendszerekkel kapcsolatos felelősségek és feladatok is változtak[22]. A „létfontosságú" kategóriába kerülés során az általános üzemeltetési feladatok mellett általános hatósági feladat a „javaslattevő-" a „kijelölő-" a „nyilvántartó" hatósági és az „ellenőrzést koordináló szerv" funkció ellátása. Ezen a területen változás, hogy:[23]

- a létfontosságú rendszer besorolási körbe tartozó honvédelmi elektronikus információs rendszerekre vonatkozóan *az ellenőrzést koordináló szerv feladatait a honvédelmi célú elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság látja el*.

[22] Ebben az összefüggésben a „rendszer" kifejezés általános jelentésű, nem csak a leszűkített „elektronikus információs rendszerekre" vonatkozik. A módosítást elrendelte: a 265/2018. (XII. 20.) Korm. rendelet a honvédelemmel összefüggő egyes kormányrendeletek módosításáról.

[23] 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről, 3. §. (2 a) és (5) pont.

– *A honvédelmi célú elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságnak új követelményként véleményezési joga van az ágazati javaslattévő hatóság döntéséhez.*

A személyes adatok védelme és a közérdekű adatok nyilvánossága – 2/2019. (I. 24.) HM utasítás

Új feladat, hogy a honvédelmi szervezetek által – az Adatvédelmi Szabályzatukban rögzített eljárás szerint – a kijelölt HM szerv felé bejelentett adatvédelmi[24] incidens ügye haladéktalanul átkerül a Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központhoz.

Az új lépés célja a bekövetkezett adatvédelmi incidens kapcsán az elektronikus információbiztonsági esemény megvalósulásának vizsgálata. A lépés tükrözéseként megjelenő követelmény, hogy az elektronikus információbiztonsági esemény vizsgálata kapcsán vélhető adatvédelmi incidens vizsgálata érdekében visszafelé történő értesítési kötelezettséget határoz meg az utasítás.[25]

Minősített adatkezelésre vonatkozó törvény – Mavtv.

A minősített adatkezelést szabályozó törvény két lényegi kérdésben változott:[26]

– A Nemzeti Biztonsági Felügyelet a minősített adatok védelmének szakmai felügyeletéért felelős miniszter (BM) irányítása alatt álló Nemzetbiztonsági Szakszolgálat keretébe került át.
– A törvény bevezette a „külföldi minősített adat" kategóriát. A Magyar Honvédség nemzetközi és hazai műveletei, gyakorlatai során keletkezett, felhasznált adat (melyek hozzáférését a felek korlátozzák) *attól függetlenül, hogy a részvevő felek között létezik-e nemzetközi megállapodás a minősített adatok védelmére*. A minősített adatokra vonatkozó rendelkezéseket a művelet, gyakorlat jellegétől függően a Magyar Honvédség – vagy az irányítást végző fél – határozza meg.
– Megjegyzés: érdekesség annak a korábban már más jogszabálynál említett követelménynek rögzítése, hogy *a hatósági feladatokat ellátó szervezet független és működése során a hatósági ügyek tekintetében nem utasítható*.

[24] Az „adatvédelem" kifejezés a hatályos jogszabályoknak megfelelően az adattartalommal, adatfelhasználással kapcsolatos eljárások rendje, ami eltér az „információvédelem" vagy „elektronikus információvédelem (biztonság)" technikai megközelítésű feladataitól.

[25] A honvédelmi miniszter 2/2019. (I. 24.) HM utasítása a személyes adatok védelmével és a közérdekű adatok nyilvánosságával összefüggő feladatok irányításáról és felügyeletéről, valamint az ezekhez kapcsolódó egyes tevékenységek eljárási rendjéről, 20. § (2-3.) p.

[26] A minősített adat védelméről szóló 2009. évi CLV. törvény, 20. és 3. §.

Minősített elektronikus adatkezelés – 161/2010. (V. 6.) Korm. rendelet

A minősített elektronikus adatkezelés területén[27] új szabályként jelent meg[28] az eseménykezelési rendszer által biztosított információs szolgáltatások és a minősített adatkezelésre felhatalmazott elektronikus információs rendszerek üzemeltetési feladatainak egy területen történő összehangolása. E szerint *az operációs rendszereket az illetékes eseménykezelő központ által kiadott riasztás esetén (de legalább havonta) frissíteni kell*.[29]

A jogszabályban meghatározott kötelezettséghez kiegészítő információ, hogy egy frissítésre vonatkozó információ nem minden esetben „riasztás" formájában publikált, illetve a frissítés gyakorisága az adott termék gyártójától függ, termékenként lényegesen eltérhet.

Remélhető, hogy ezt a kezdeti lépést további összehangolási lépések követik annak érdekében, hogy *a minősített elektronikus adatkezelés és a nem minősített („nyílt") adatkezelés összehangolása technikai szinten is megtörténjen a jogszabályokban.*

A honvédelemről szóló törvény - Hvtv.

A honvédelem alapvető kérdéseit meghatározó sarkalatos törvény[30] a kibertér műveletek szempontjából lényegi változásokat tartalmaz:[31]

- A felhasználásra vonatkozó pontosítás szerint a Honvédség felhasználható (ami eltérés a fegyveres erőként való alkalmazástól erőszakos cselekmények, kibertérből érkező vagy elektronikai támadások, fenyegetések elhárítására két különleges jogrendi időszak esetén (szükségállapot és terrorveszély).
- A „műveleti terület" értelmezése megváltozott, *a korábbi megfogalmazás szerinti műveleti tervekben meghatározott terület és a felette levő légtér mellett már tartalmazza a kiberteret is*, ami a nemzeti és szövetségi alkalmazhatóság alapvető lépése a NATO Varsói Csúcsértekezlet műveleti területtel kapcsolatos döntésével összhangban.[32]

---

27 A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet.

28 323/2018. (XII. 28.) Korm. rendelet az egyes belügyi tárgyú és más kapcsolódó törvények módosításáról szóló 2018. évi CXXI. törvénnyel összefüggő Korm. rendeletek módosításáról, 13. §.

29 161/2010. (V. 6.) Korm. rendelet 34/A. §.

30 A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény, 80. § (5) pont; 80. § (22) pont, és 21/A. § (6) d) pont.

31 A változásokat az egyes törvényeknek a Magyar Honvédség új szervezeti rendjének kialakításával összefüggő módosításáról szóló 2018. évi CX. törvény rendelte el 2019. 01. 01-től.

32 ...„recognise cyberspace as a domain of operations"...; Warsaw Summit Communiqué 70. p; https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

– *Megjelent a „honvédelmi vészhelyzet" állapot*, ami a különleges jogrendi helyzetek előtti időszakban alkalmazható szomszédos államban kialakult, katonai kezelést igénylő, hazánkat közvetlenül érintő fenyegetés vagy szövetségesi kötelezettség teljesítésére vonatkozó felkészülés érdekében. Kibertér területű vonatkozás, hogy *a vészhelyzet megoldásához a Katonai Nemzetbiztonsági Szolgálat és a honvédségi szervezetek felderítő, elhárító, valamint kibertér műveleti erői tevékenysége fokozható* (a fenyegetettség hazánkra történő átterjedése, felerősödésének megakadályozása érdekében).

Végrehajtási rendelet szintű feladatok – 290/2011. (XII. 22.) Korm. rendelet

Az előzőekben megfogalmazott, kibertér műveleti szempontból alapvetőnek tekinthető felhatalmazás és követelménytámasztás végrehatása nem tekinthető egy lépésben megoldható feladatnak. A Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program által tervezett technikai fejlesztési lépések, szervezési, képzési és egyéb feladatok együttese eredményezhet valós, kibertér műveleti területen is értékelhető eredményeket.

A szervezetátalakítás során új, előzmények nélküli követelmény, hogy a Honvédségnél megjelent a kiberműveleti tevékenység, a katonai műveletek kibertérben történő támogatásának feladata szoros együttműködésben a jogszabályban meghatározott honvédelmi ágazati tevékenységgel.[33]

Fontosabb NATO szempontok

A brüsszeli NATO Csúcstalálkozó[34] megerősítette, hogy a NATO célja a hatékony működés a kibertérben, hasonlóan a földi, vízi vagy légi műveletekhez. Politikai felügyelettel *integrálni kell a szövetségesek által felajánlott kibertér hatásokat a NATO műveleteibe, misszióiba*.

A szövetségesek eltökéltek az erős nemzeti kibervédelem kialakításában, a NATO Kibervédelmi Képességvállalás teljesítésével (ellenállóképesség fokozása, illetve az ellenséges kibertámadások költségesség tétele).

A NATO kiegészíti a parancsnoki struktúrát egy új szervezeti elem felállításával 2018. augusztus 1-jei kezdettel (Kibertér Műveleti Központ – Cyberspace Operations Centre) a katonai döntésekhez szükséges kibertér helyzetkép biztosítása, a NATO és szövetségi erők összehangolása, a műveletek szabadságának biztosítása (freedom of operations) érdekében.

---

[33] 290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról, 11. §. 23. pont.

[34] NATO Brüsszeli Csúcstalálkozó Deklaráció, 2018. július 11-12; 20, 29. pont. https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Letöltés ideje:

A tagállamok a kártékony kibertér tevékenységek jellemzőinek azonosítása (attribution) után összehangolhatják válaszlépéseiket, de *az azonosítás feladata független nemzeti ügynek tekintendő*.

A NATO tagállamok megerősítik szándékukat, hogy *a kibertér műveletek továbbra is a nemzetközi normák betartásával történhetnek*.

A NATO Kibertér Műveleti Központ tagjának publikálása szerint[35] a szervezet alapvető feladata *a kibertér helyzetismeret biztosítása, a kibertér szempontok bedolgozása a Szövetségi műveletekbe, illetve a műveleti irányítás megvalósítása minden műveleti területen*, ahol a kibertér hatások érvényesülhetnek a manőverek szabadságának biztosítása érdekében. A Központ feladatait stratégiai és hadműveleti szinten látja el, illetve összekötő szerepet lát el a nemzetek irányában, információmegosztással szolgálja a szükséges helyzetismeretet, beleértve kihelyezett koordinációs elem alkalmazását is.

A 2019. február 12-13-i NATO védelmi miniszteri találkozó után kiadott tájékoztatás[36] megfogalmazza, hogy az említett Kibertér Műveleti Központ 2023-ra éri el a teljes készenlétet.

A NATO nem tervezi saját offenzív kibertér képességek kialakítását. A tagállamok önkéntes alapon felajánlhatják saját képességeiket (sovereign cyber effects) a NATO műveletek és missziók érdekében. Több nemzet már felajánlotta képességeit; ilyen esetekben *az adott nemzet teljes felügyeletében maradnak ezek a képességek*.

EU „Kiberbiztonsági Jogszabály" (Cybersecurity Act) javaslat – jövőbeli feladatok

A rövid időn belül megjelenő jogszabálytervezet[37] kettős célt szolgál: részletezett funkció, feladatok, felépítés, erőforrások meghatározásával rendezi az Európai Uniós Kiberbiztonsági Ügynökség (továbbiakban: Ügynökség) jövőjét, illetve hiánypótlásként kialakítja, bevezeti az európai infokommunikációs technológiák tanúsításával kapcsolatos megoldást és tanúsítási keretrendszert.

Az első témakör szükségességét az okozza, hogy a 2004-ben megalakult Ügynökség mandátuma 2020-ban lejár, így rendezni kell ennek a funkciónak a sorsát. A tanúsítás témaköre EU-s szinten még nem megoldott, egyes nemzeti vagy

---

35 Don LEWIS: What Is NATO Really Doing in Cyberspace? https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/ (Letöltés ideje:

36 NATO Védelmi Miniszteri Értekezlet 2019. 02. 12-13, tájékoztató https://www.nato.int/cps/en/natohq/events_163237.htm?selectedLocale=enFact Sheet - NATO Cyber Defence (February 2019) (Letöltés ideje:

37 AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály") COM(2017) 477 final/3, Brüsszel, 2018.2.22. (javaslat)

csoportos tanúsítási megoldásokra (tanúsítványokra – certification) támaszkodhatnak a tagállamok és EU szervezetek. A saját (nemzeti) tanúsítás kérdése hazákban is megoldatlan, Magyarországon az említett tanúsító szervezetek tanúsítványainak alkalmazása (elfogadása) történik.[38]

A szabályozási elgondolás egyértelműen köthető a feljebb említett NIS Directive feladatrendszeréhez, egyrészt az ott részletezett EU-szintű eseménykezelési rend („CSIRT-ek hálózata") EU oldalról történő szakmai támogatásával, másrészt a tanúsított termékek, szolgáltatások által a biztonsági szint megerősítésével.

Az Ügynökségnek nem feladata az eseménykezelés vagy biztonsági vizsgálat. Szakmai támogató szervezetként egyrészt az EU-s szabályozási, szakpolitikai folyamatokat támogatja, tanácsadó szerepet tölt be, kutatásokat támogat (kulcskérdés a korszerű szakértői háttér kialakítása és folyamatos fejlesztése), másrészt a nemzetek felé konzultációs fórumot biztosít, tanácsokat ad (pl. eseménykezelés vagy oktatási rendszer struktúrájának kialakításában), közvetítő szerepet játszik, képzéseket alakít ki, kibervédelmi gyakorlatokat szervez.

Lényegi kérdés, hogy *az Ügynökség semmilyen felügyeleti, hatósági szerepkörrel nem rendelkezik* EU szinten, illetve ugyanígy *nem érinti a tagállamok saját hatósági, eseménykezelési, szabályozási vagy egyéb önállóságát*.[39]

Az Ügynökség katonai kérdésekkel nem foglalkozik, de már EU szinten is egyre erőteljesebb a civil-katonai együttműködés kérdése (benne a megkötött NATO – EU-szintű technikai együttműködéssel), így a képességfejlesztés, oktatás és képzés, az EU-szintű válságkezelési és kibervédelmi gyakorlatok vonalán a feladatok növekedése várható. Hazánk képviseletét ebben a rendszerben a Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet látja el.

A korábbi gyakorlatnak megfelelően ezen a vonalon kerülnek hazánkba az említett szakmai kérdések, illetve a Nemzeti Kibervédelmi Intézet szervezésében történik a hazai szakfeladatok szervezése (szabályozási kérdések, biztonságtudatossági rendezvények – mint az októberi Kiberbiztonsági Hónap, regionális és EU-s gyakorlatokon való részvétel, illetve a nemzeti szintű gyakorlatok rendjének kialakítása) és megtörténik a honvédelmi ágazattal történő összekapcsolás. A napi gyakorlatban ugyanezen a vonalon zajlik a már említett jogszabályok rendje szerint az eseménykezelő rendszerek együttműködése.

Az Ügynökség feladata lesz az EU-szintű tanúsítási keretrendszer kialakítása és fejlesztése egy háromfokozatú rend kialakításával („alapvető", „jelentős" és „magas" biztonsági szint szerinti tanúsítás). Minden nemzetnek tanúsításfelügyeleti hatóságot kell azonosítania a nemzeti feladatok felügyelete érdekében. A nemzeti

---

[38] A tanulmány témájától eltérő, de hasonló jelenség azonosítható a minősített elektronikus adatkezeléshez szükséges rejtjelző eszközök és megoldások területén. A saját nemzeti megoldások mellett a nemzetközi hálózatok, vagy közös szervezetek rejtjelzését „Titkos" vagy magasabb minősítés esetén NATO által akkreditált rejtjelző eszközökkel lehet megoldani. EU minősített adat esetén más akkreditálási szisztéma működik, de ugyanúgy nemzeti tanúsított (akkreditált) eszköz vagy megoldás nemzetközi átvétele történik.

[39] II. cím, 4-11. cikk.

tanúsításfelügyeleti hatóságok képviselőiből megalakul az európai tanúsításfelügyeleti csoport egyrészt az EU-s döntések szakmai támogatása, másrészt a tanúsítási keretrendszer kialakítása érdekében.[40] A tanúsítással kapcsolatos technikai vetületű, a kialakítás előzményeit is összefoglaló írás Tóth Tamás tollából részletesebb információt szolgáltat erről a témáról,[41] így további ismertetésre nincs szükség ebben a tanulmányban.

A tanúsítással kapcsolatos feladatok hazánkban e szerint új hatósági feladat megjelenését eredményezik, illetve a megkezdődő EU-szintű keretrendszer kialakításához napi szintű bedolgozó, szakmai támogatást kell biztosítani.

Új kihívást, azonnali *nemzeti szintű szabályozási feladatot jelent a várhatóan megjelenő „alapvető", „jelentős" és „magas" biztonsági szintű tanúsított termékekre vonatkozó követelmény*, mivel a jelenlegi, hálózatok biztonsági besorolására vonatkozó 5-ös skálát meg kell feleltetni ennek a hármas besorolásnak. Ezt csak akkor lehet megoldani, ha a biztonsági osztályba soroláshoz szükséges kockázatelemzési módszertanok és eljárások átdolgozása megtörténik, kialakul, hogy milyen fenyegetési szinthez melyik biztonsági osztályhoz illeszkedő melyik tanúsítási szintet kell alkalmazni. Ez a feladat a honvédelmi ágazat, a honvédelmi elektronikus információs rendszerek területén azonnal jelentkezni fog, beleértve azt a kérdést is, hogy a kockázatelemzésre vonatkozó kérdések az eddigihez hasonlóan maradnak-e ágazati hatáskörben, vagy legalább irányelv-szinten centralizáció kezdődik ezen a területen.

Az esetlegesen megjelenő, tanúsított termékek alkalmazására vonatkozó követelmény már az első lépésnél költségvetési igényeket fog generálni, ahogy erre Tóth Tamás is rámutatott a korábban hivatkozott írásban. Az állami és önkormányzati szervezetek nyílt és minősített adatait kezelő rendszerei a létfontosságú infrastruktúra elemek (benne a honvédelmi célból kijelölt rendszerek) esetében jelentős költségeket, illetve technikai feladatokat fog jelenteni a tanúsított termékek alkalmazásával kapcsolatos kötelezettségek megjelenésével. Emiatt *kritikus fontosságú, hogy a jogszabályok módosításának előkészítése során a jogszabályalkotó valóban mérje fel a változásokkal kapcsolatos költségeket, de nem csak a központi funkciók kialakítására vonatkozóan*. A létfontosságú infrastruktúra, kormányzati rendszerek, a honvédelmi elektronikus információs rendszerek területén megjelenő új igények tárcák által történő „kigazdálkodása" ekkora feladatok esetén nem lehetséges, így már a kezdeteknél központi költségvetési támogatásra lesz szükség.

Éves honvédelmi miniszteri feladatszabás (2019)

Az eddig azonosított, a hálózatbiztonsági vagy kibertér műveleti képességekre hatással bíró nemzetközi követelmények, irányok, vagy jogszabályi változások

[40] III. cím, cikk 45-48, 50, 53. cikk.

[41] TÓTH Tamás: Az Európai Unió kiberbiztonsági tanúsítási keretrendszere; Szakmai Szemle, 2019/1. pp. 97-115.

honvédelmi területen a 2019-es évi miniszteri feladatmeghatározás szerint az alábbi területeken képeznek kihívásokat:[42]

- Éves kiemelt feladat *a Nemzeti Biztonsági Stratégia felülvizsgálata*,[43] erre alapozva *a Nemzeti Katonai Stratégia felülvizsgálata*, és ennek kapcsán *az alacsonyabb szintű katonai szabályozók*[44] kidolgozása. A két dokumentum 2013-as kiadású, így nyilvánvaló, hogy a katonai kibertér műveletek területén (figyelemmel a Hvtv. korábban említett változására) alapvető változások várhatók.
- *Folytatni kell a honvédelmi ágazati szintű elektronikus eseménykezelésre, sérülékenység-vizsgálatra és hatósági felügyeleti funkciókra vonatkozó képességfejlesztést.* Ehhez kapcsolódik a honvédelmi feladatokat támogató híradó-informatikai infrastruktúra fejlesztésre, az ezt támogató kibertér műveleti képességfejlesztésre-,[45] illetve a honvédelmi szervezetek információvédelmének fejlesztésére vonatkozó feladatszabás. *Folytatni kell az EU Állandó Strukturált Együttműködés keretén belül történő fejlesztéseket* (e területen kibervédelmi szakfeladatok is azonosíthatók). Fontos feladat a nemzetközi (EU, NATO) és nemzeti gyakorlatokon való részvétel, ami mindhárom területen tartalmazza a kibervédelmi gyakorlatokat is.
- A 2020-2021. évi iránymeghatározás az éves feladatszabás folytatása. Önálló elemként megjelenik *a honvédelmi létfontosságú rendszerelemek kijelölésére irányuló hatósági eljárások lefolytatása*. Ez a korábban említett jogszabályok változásai miatt honvédelmi ágazati kijelölt hatóságra vonatkozó szakfeladatot is jelent, illetve a kijelölés mellett a nyilvántartási és ellenőrzési feladatokat is módosítani kell.

Összefoglalás

Az áttekintett források egyértelműen jelzik a kibertérben történő műveletek bonyolultságának növekedését. A fenyegetések és az általuk bekövetkező veszélyek szintjének emelése válaszként megköveteli a védelmi rendszabályok, eljárások továbbfejlesztését nemzetközi (pl. EU- és NATO-szinten) és nemzeti szinten egyaránt. Ennek megfelelően *várható a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálási rendszer kialakulása és fejlődése*.

---

[42] A honvédelmi miniszter 3/2019. (I. 31.) HM utasítása a honvédelmi szervezetek 2019. évi feladatainak, valamint a 2020–2021. évi tevékenysége fő irányainak meghatározásáról, 2. §. 16. p; 3. §. 9-11. p; 26. p; 29. p; 4. §. 5. p; 8. p és 40. p.

[43] A stratégiai dokumentumok egymásra épülése és a Nemzeti Biztonsági Stratégiában megfogalmazott általános feladatok szakmai stratégiában szükséges továbbbontása feltételezi a 2013-as Nemzeti Kiberbiztonsági Stratégia felülvizsgálatát is.

[44] Alapvető fontosságú a doktrinális kérdések rendezése. Ennek első lépése a 2019-ben várható NATO Kibertér Műveleti Doktrína megjelenése, magyar ratifikálása, illetve az illeszkedő nemzeti feladatok megfogalmazási szintjével, formájával kapcsolatos döntések gyors meghozatala.

[45] Szervezeti szempontból kiemelt jelentőségű, hogy az új szervezeti struktúrában a Magyar Honvédség Parancsnoksága kibervédelmi szervezeti elemet (Kibervédelmi Szemlélő) tartalmaz, melynek fő feladata a stratégiai szintű feladatok menedzselése, a jövőbeli képességfejlesztés irányainak meghatározása.

Nemzetközi és nemzeti szinten egyaránt megfogalmazott cél a különböző témák szerint csoportosított kibervédelmi gyakorlatokban rejlő lehetőségek kihasználása, ami a technikai képességfejlesztés, tapasztalatszerzés mellett nyomatékosan tartalmazza az együttműködés, információcsere gyakorlási és fejlesztési feladatait, beleértve a civil-katonai együttműködés erősítését.

A honvédelmi tárcának éves kiszabott feladatot jelent a nemzeti biztonsági és a katonai stratégia felülvizsgálata, a hat év alatt felhalmozódott tapasztalatok átvezetése. Ehhez *a feladathoz tartozik a stratégiai és hadműveleti szintű szabályozók kidolgozása, ahol elsőbbséggel kell említeni a kibertér műveleti doktrinális kérdések komplex megoldását* (NATO doktrína ratifikálása, szükség esetén saját nemzeti feladatokat meghatározó dokumentum kiadása, illetve a magyar Doktrína Hierarchia dokumentumaiban a kibertér műveleti kérdések átvezetése).

A jogszabályokban megfogalmazott korai előrejelző rendszer kialakítása remélhetően nagyságrendi javulást eredményez a védelem hatékonyságában. *A honvédelmi célú elektronikus információs rendszereknél ki kell alakítani ezt a védelmi mechanizmust, figyelembe véve a katonai sajátosságokat, ezzel párhuzamosan szorosan együtt kell működni és közösen kell fejlődődni a központi szolgáltatásokat biztosító megoldásokkal.*

A honvédelmi létfontosságú infrastruktúravédelemre vonatkozó szabályozás változása megteremti a lehetőséget, hogy *a különböző jogszabályok szerinti üzemeltetési és védelmi rendszabályok kialakítása és menedzselése egységes szemlélettel történjen, ami az üzemeltető szervezetek számára csak előnyökkel járhat*.

A kibervédelmi terméktanúsításra vonatkozó EU-szintű változás nyomán a nemzeti szabályozás, biztonsági követelmények is változni fognak, melyre meg kell tenni a lehetséges szakmai előkészületi lépéseket.

A honvédelmi ágazatnál eseménykezelés területén technikai területű, fejlesztést és szervezést igénylő változást jelent a sérülékenységvizsgálatok témakörének bővülése, illetve az adatvédelmi területtel történő szoros technikai területű központi követelmény.

A honvédelmi feladatszabással kapcsolatban komoly szakmai vizsgálatot igénylő kérdés annak eldöntése, hogy a fentiekben vázolt keretrendszer, a legújabb változások ismeretében milyen formában, milyen állami, jogi eszközzel kell kijelölni, meghatározni a katonai kibertér műveleti képességeket. A kérdés konkrétan így fogalmazható meg: *a tervezett nemzeti szintű biztonsági stratégia és a katonai stratégia felülvizsgálat gondolati vonalába beilleszthető-e egy nemzeti katonai kibertér műveleti stratégia megfogalmazása, kialakítása és tartalmi elemeinek feladatként történő elrendelése, tekintettel a nemzeti katonai védelmi feladatokra, egyben a nemzetközi kötelezettségvállalások teljesítésére?* A kérdést nem ez az írás, hanem a jövőbeli történések fogják megválaszolni…

A tanulmány befejező mondata köszönet a kollégák, barátok, civil és katonai szakértők, fiatal kutatók felé, aki támogatták annak megjelenéséhez szükséges keretek körvonalazását, lényegi elemek azonosítását.

Felhasznált irodalom:

- A BIZOTTSÁG AJÁNLÁSA (2017. 09. 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról, C(2017) 6100 final, Brüsszel, 2017. 09. 13.
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály") COM(2017) 477 final/3, Brüsszel, 2018.2.22. (javaslat)
- Don LEWIS: What Is NATO Really Doing in Cyberspace? https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/ (Letöltés ideje: 2019. 02. 28.)
- EU Cyber Defence Policy Framework (2018 update) Brussels, 19 November 2018 (OR. en) 14413/18.
- KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése, Brüsszel, 2017.9.13. JOIN(2017) 450 final
- TÓTH Tamás: Az Európai Unió kiberbiztonsági tanúsítási keretrendszere; Szakmai Szemle, 2019/1. pp. 97-115.
- NATO Büsszeli Csúcstalálkozó Deklaráció, 2018. július 11-12.
- NATO Védelmi Miniszteri Értekezlet 2019. 02. 12-13, tájékoztató
- NATO Warsaw Summit Communiqué (2016)
- Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája (2018)

Felhasznált jogszabályok:

- 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről
- 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól
- 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról

- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságokra, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 2/2019. (I. 24.) HM utasítás a személyes adatok védelmével és a közérdekű adatok nyilvánosságával összefüggő feladatok irányításáról és felügyeletéről, valamint az ezekhez kapcsolódó egyes tevékenységek eljárási rendjéről
- 2009. évi CLV. törvény a minősített adat védelméről
- 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat szabályairól
- 290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról
- 3/2019. (I. 31.) HM utasítás a honvédelmi szervezetek 2019. évi feladatainak, valamint a 2020–2021. évi tevékenysége fő irányainak meghatározásáról
- 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről

BEDERNA ZSOLT

BIZALOM ÉS MEGBÍZHATÓSÁG

Bevezetés

Az Európai Unió 2013-ban kiadásra került kiberstratégiájának fő céljai és elvei, azaz a megbízható, biztonságos és nyitott kiber-ökoszisztéma elősegítése, továbbra is érvényben vannak. Azonban az Unió feltett szándéka a kiberbiztonsággal kapcsolatosan az ellenállóképesség, az elrettentés és a védelmi képességek hatékonyságának növelése[1], melyek elérésében a többrétegű és a többszereplős működési modell[2] alkalmazása okoz nehézséget. Ennek megfelelően annak egyik sarPCIontja a szereplők közötti, valamint a velük kapcsolatba hozható tényezőkre vonatkozóan (pl. alkalmazott technológia) a bizalom fejlesztése.

Azonban az elmúlt évek tapasztalatai alapján ez korántsem egyszerűen kivitelezhető feladat. A megfelelő bizalmi szint elérése és fenntartása egy szervezet szempontjából folyamatos jellegű tevékenységet kíván meg. A teljes életciklus során minden erőforrás esetén szükséges a megfelelő bizalmi szint felmérése, fenntartása és visszamérése.

A NIST[3] SP[4] 800-39 nyomán a bizalom objektív eredményen és szubjektív véleményen alapuló, tapasztalati úton szerzett vagy szabály által kötelező jellegű hiedelem, hogy egy entitás (állam, szervezet, egyén, eszköz, folyamat stb.) viselkedése vagy működése az előre jelzett mód szerint valósul meg[5].

A bizalom tehát egy olyan érzet, amely objektív és szubjektív összetevőből származik. A szubjektivitás az egyéni, szervezeti szinten a környezet és a média által befolyásolt kialakult érzet, konformitási és használhatósági szint alapján keletkezik. Azonban az objektivitás kezelése ennél összetettebb kérdéskör, mely egy belső vagy külső, független tesztelési (validációs vagy verifikációs) eljárás kimenete.

Az ISO/IEC/IEEE 15288:2015[6] definíciója alapján a validáció az a folyamat, amely által szavatolásra kerül, hogy egy termék, szolgáltatás vagy rendszer stb. a felhasználói (megrendelői) elvárásoknak megfelelően került megalkotásra. A verifikáció az a folyamat, amely által értékelésre kerül, hogy egy termék,

---

1 AZ UNIÓ KÜLÜGYI ÉS BIZTONSÁGPOLITIKAI FŐKÉPVISELŐJE: KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése, Brüsszel: EURÓPAI BIZOTTSÁG, 2017.

2 Annegret BENDIEK: European Cyber Security Policy, SWP Research Paper, 2012., p. 12.

3 National Institute of Standards and Technology

4 Special Publication

5 NIST: Managing Information Security Risk, https://doi.org/10.6028/NIST.SP.800-39, p. 24. (Letöltés ideje: 2016. 03. 05.)

6 ISO/IEC/IEEE 15288:2015 Systems and Software Engineering, International Organization for Standardization, 2015.

szolgáltatás vagy rendszer stb. a specifikációnak, szabályozásnak és egyéb követelményeknek megfelelően került megalkotásra.

A megbízhatóság – hasonlóképp a NIST SP800-39 nyomán – egy entitás olyan jellemzője (attribútuma), amely más entitások számára bizonyítja, hogy rendelkezik egy adott feladat sikeres elvégzéséhez a szükséges és elégséges kvalitással és képességgel, ezáltal emelve a felé irányuló bizalom szintjét[7].

A bizalom kialakításának lehetőségeit a rendelkezésre álló bizalmi modellek határozzák meg, valamint a bizalmi szint kialakításában a megbízhatósági jellemző megállapítása kulcsfontosságú. Ennek megfelelően a továbbiakban e két kérdéskört tárgyalom.

Bizalmi modellek

A bizalom definíciójából kiindulva, a bizalmi kapcsolatok kialakítása (és fenntartása) nem egyértelmű, bonyolult folyamat, mely a szubjektív összetevő következtében eltérő értelmezést és ennek következtében eltérő megoldást takarhat mindenki számára.

A bizalmi modellek e problémakört hivatottak leegyszerűsíteni azáltal, hogy az egyes modellek a bizalmi kapcsolat kialakításának módját, jellegét határozzák meg. Ezen túlmenően az alkalmazott modell definiálja (vagy legalább befolyásolja) az információáramlást és az információ-megosztás jellegét, mértékét, valamint az informatikai és információbiztonsági szolgáltatások kialakításának, megvalósításának jellegét, továbbá a tranzitivitás kérdésére is választ adhat. Ez utóbbi az alkalmazott modell függvényében egyaránt lehet egyén- és szituációfüggő, vagy szerződésben, akár jogszabályi szinten egyaránt meghatározott.

A bizalmi modellek között hasznosság, alkalmazhatóság szerint nem lehet különbséget tenni, az adott modell megfelelősége szituációfüggő (pl. szervezeti és irányítási struktúra, kockázati étvágy, adatok érzékenysége stb. következtében). A NIST SP800-39 által meghatározott modellek az alábbiak[8]:

- Validált bizalmi modell (Validated trust),
- Közvetlen történeti bizalmi modell (Direct historical trust),
- Közvetített bizalmi modell (Mediated trust),
- Kötelező bizalmi modell (Mandated trust),
- Hibrid bizalmi modell (Hybrid trust).

A validált bizalmi modell esetén a megbízó fél a rendelkezésre álló bizonyítékok alapján ellenőrzi a megbízandó fél megbízhatóságát, vagy ezáltal felülvizsgálja a már meglévő bizalmi kapcsolatot. A külső fél általi validálás auditálás útján kialakított megbízhatósági érték hozzárendelését takarja az auditált külső félhez. Azonban ez korlátozott esetekben kivitelezhető folyamat, minthogy a legtöbb szervezet a külső fél által végzett validálás folyamatához legfeljebb

[7] NIST: Managing Information Security Risk, https://doi.org/10.6028/NIST.SP.800-39, p. 24. (Letöltés ideje: 2016. 03. 05.)

[8] NIST: Managing Information Security Risk, https://doi.org/10.6028/NIST.SP.800-39, pp. G-1 – G-3. (Letöltés ideje: 2016. 03. 05.)

részlegesen vagy egyáltalán nem szolgáltat belső információt, ennél fogva a bizonyítékok beszerzése jelenti a problémát. E problémakör feloldását célozza a közvetlen történeti és a közvetített bizalmi modell egyaránt.

A közvetlen történeti bizalmi modell a múltbeli közvetlen együttműködés, más szervezettel történő együttműködés eredménye, kimenete, egyéb események alapján empirikus úton megalkotott bizalmi kapcsolat létrehozását és fenntartását írja le. A múltbeli események, tapasztalatok láncolata a bizalmi szintet pozitív vagy negatív irányba egyaránt elmozdíthatják.

A közvetített bizalmi modell esetén két szervezet között egy mindkét fél által bizalmi kapcsolatban lévő szervezet közvetítésével valósul meg a bizalmi kapcsolat kiépítése, mely időben történhet egyszerre vagy egymáshoz képest eltolva. A közvetített bizalom megvalósítására példa egy nemzetközi szabvány szerinti érvényes, külső fél által végzett tanúsítás (pl. ISO/IEC 9001:2015[9], ISO/IEC 27001:2013[10], Payment Card Industry Data Security Standard szabvány[11] stb. alapján).

A kötelező bizalmi modell esetén a megbízó fél a bizalmi kapcsolat létrehozására egy, az adott entitás számára az érintett témakörben, tevékenységi körben vagy iparágban jogkörrel és hatáskörrel bíró másik entitás által kötelezett.

A hibrid bizalmi modell olyan esetben nyújt segítséget, amely esetén más egyéb kategória nem alkalmazható egyértelműen. A modellek ugyanis nem egymást kizáró jellegűek, akár önállóan, akár más modellel keverve egyszerre alkalmazhatóak.

E modelleket a NIST alapvetően a szervezetek közötti bizalom fél-formális leírásaként publikálta. Azonban, mint ahogy a következő fejezetekben látni fogjuk, e modellek alkalmazása további alapvető szervezeti tényezőkön, összetevőkön keresztül is lehetséges.

A megbízhatóság kérdésköre

A bizalom vonatkozásában, annak jellege következtében nem alakítható ki explicit értékelési rendszer, azonban a megbízhatóság tekintetében az egyes entitásokat jellemezhetjük kvalitatív vagy kvantitatív megbízhatósági értékekkel. E megállapításból kiindulva, a kialakított értékelési skála szerint (függetlenül annak kvalitatív vagy kvantitatív jellegétől) szükség szerint létrehozható egy megbízhatósági sorrend is.

---

9 ISO/IEC 9001:2015, International Organization for Standardization, 2015.

10 ISO/IEC 27001:2013. Information technology – Security Techniques – Information security management systems — Requirements, International Organization for Standardization , 2013.

11 PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1549211879330 (Letöltés ideje: 2019. 02. 03.)

Az ISACA[12] nemzetközi szervezet információbiztonságra vonatkozó BMIS[13] üzleti modellje négy elemből tevődik össze. E komponensek az emberi tényező, a folyamat, a szervezet és a technológia, amelyeket hat dinamikus jellegű kapcsolat köt össze, azaz a kultúra, az irányítás, az architektúra, az érvényesülés, a felhatalmazás, a támogatás, valamint az emberi tényező. Ezek biztosítják, hogy az egyik tényező változása a többi tényező változását is magával vonja[14].

A BMIS modellt megvizsgálva, egyértelmű következtetés vonható le, hogy a modell négy statikus összetevőjéhez, mint a működést alapvetően meghatározó tényezőhöz hozzárendelhető egy megbízhatósági viszonyszám, amely az adott összetevő felé kialakított bizalom szintjét befolyásolhatja (pozitív irányban) más entitások részéről.

Az emberi tényező megbízhatósága

Abból a tényből kiindulva, hogy egy szervezetet emberek alkotják, akik az adott szervezet folyamatait tervezik és működtetik, továbbá a folyamatok végrehajtása során emberek által megtervezett, létrehozott és működtetett technológiai erőforrásokat használnak, az emberi tényező képessége, tudása, hozzáállása alapvetően meghatározza a másik három elem működését. Az emberi tényező bizalmi szintje kritikus fontossággal bír az egész ökoszisztémára vonatkozóan. Az összefüggés jellege egyenes arányosságon alapul, azaz az emberi tényező pozitív teljesítménye pozitív hatással bír, míg a negatív teljesítmény szándékolt vagy nem szándékolt károkozás formájában negatív hatást eredményez.

Az emberi tényező megbízhatóságát a felvételkor és a munkavégzésével kapcsolatosan a jogszabályi kereteken belül maradva szükséges ellenőrizni. A személyes adatok kezelését a 2016. április 27-én hatályba lépett, 2018. május 25-től alkalmazandó *az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)*, azaz GDPR (General Data Protection Regulation) egységesen szabályozza az Európai Unióban. (Az Általános adatvédelmi rendelet alapján kialakított Adatvédelmi irányítási rendszer (ADIR) és az Információbiztonsági irányítási rendszer (IBIR) szoros kapcsolatot mutat, amelyet a Szakmai Szemle XVI. évfolyam 3. számban megjelent cikkemben vizsgáltam[15].) A magyarországi sajátosságokat *az információs önrendelkezési jogról és az információszabadságról* szóló 2011. évi CXII. törvény tartalmazza.

A munkaerő felvételekor bevett eljárás az önéletrajz-alapú szelekció, amely a validált bizalmi modellt valósítja meg. Ezen túlmenően a büntetlen előélet igazolása jogszabályban meghatározott esetekben kérhető hatósági erkölcsi bizonyítvány bemutatásával, amelyet *a munka törvénykönyvéről* szóló 2012. évi I. törvény 44/A. § szabályoz. *A nemzetbiztonsági szolgálatokról* szóló 1995. évi CXXV. törvény 74. § tartalmazza a nemzetbiztonsági átvilágítás alá eső személyek körét. Hasonló

[12] Information Systems Audit and Control Association
[13] Business Model for Information Security
[14] ISACA: The Business Model for Information Security, ISACA, 2010., pp. 13-46.
[15] BEDERNA Zsolt: Az Általános adatvédelmi rendelet és az információbiztonság kapcsolódási pontjai, Szakmai Szemle, 2018/3. pp. 76-103.

ellenőrzést a nemzeti minősített adatok esetén is le kell folytatni *a minősített adat védelméről* szóló 2009. évi CLV. törvény szerint.

Az informatikai, illetve információ- és informatikai biztonság területén dolgozó szakemberek és az általuk képviselt tudás megbízhatóságának értékelésére az érintett szakterületen megszerezhető minősítések birtoklása jelenti a megbízhatósági paramétert. A minősítések vagy épp az erkölcsi bizonyítvány a közvetített bizalmi modellt valósítják meg.

Az üzleti és a támogatói folyamatok működtetése, azaz az operatív működés során az emberi tényezővel kapcsolatos biztonság és ezzel a bizalom szintjének fenntartása szükségszerű, amelyre az oktatás és tudatosítás a kézenfekvő megoldás. A munkatársak tudása (oktatás-visszamérés) és attitűdje (kontrollok működése) leképezhető egy tetszőleges érettségi modellre (pl. SANS érettségi modellje[16]), amely a validált bizalmi modellnek feleltethető meg.

A folyamatok megbízhatósága

Egy folyamatot a végrehajtása által elért eredményeken, azok reprodukálhatóságán keresztül, valamint az adott folyamatlépéseken értelmezett mérőszámokkal lehetséges mérni. Jellemzésük, érettségi szintjük megállapítása az érettségi modellek alkalmazásával lehetséges.

Az ISACA által megalkotott informatikai irányítási és menedzsment, valamint az operatív folyamatokat leíró COBIT[17] modell[18] szerves részét képezi a PAM[19] folyamatképességet leíró modell[20]. A PAM az ISO/IEC 15504 szabványnak[21] felel meg, amely 2015-ben az ISO/IEC 33001 szabványt[22] írta felül.

A COBIT folyamatképesség-modellje alapján a folyamatokat a folyamatképességek figyelembevétele mellett egy hatos skálán lehetséges minősíteni[23]:

- Hiányos (0) a folyamat, ha nem implementált vagy nem éri el a célját.
- Végrehajtott (1) a folyamat, ha teljesíti a céljait azáltal, hogy a bemenet alapján végrehajtott részfeladatok végrehajtása útján előállnak a kimeneti termékek.
- Irányított (2) a folyamat, ha végrehajtása tervezett, felügyelt és szabályozott módon történik, biztosítva ezáltal, hogy a célkitűzések teljesítésével

---

16 Lance SPITZNER: Defining the Security Awareness Maturity Model, https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model (Letöltés ideje: 2018. 05. 09.).

17 Control Objectives for Information and Related Technologies

18 ISACA: COBIT 5, 2012.

19 Process Assessment Model

20 ISACA: Process Assessment Model (PAM): Using COBIT 5, 2013.

21 ISO/IEC 15504:2013. Information technology – Process assessment, International Organization for Standardization, 2013.

22 ISO/IEC 33001 Information technology – Process assessment – Concepts and terminology, International Organization for Standardization, 2015.

23 ISACA: Process Assessment Model (PAM): Using COBIT 5, 2013. p. 13.

megfelelően kialakított, kontrollált és karbantartott eredménytermékeket eredményezzen.

- Kialakított (3) a folyamat, ha az irányított folyamat formálisan meghatározott és alkalmas arra, hogy a folyamat megvalósítsa a kitűzött eredményeit.
- Kiszámítható (4) a folyamat, ha a kialakított folyamat végrehajtása mérésekből származó mennyiségi információk alapján valósul meg, ezáltal biztosítva, hogy annak eredménytermékei meghatározott határértékeken belül legyenek.
- Optimalizáló (5) a folyamat, ha a kiszámítható folyamatra vonatkozóan a jelenlegi és prognosztizált üzleti célok állandó jelleggel figyelemmel kísértek, valamint a megismert információk alapján biztosított és megvalósított a folyamatos fejlesztés.

Összességében megállapítható, hogy egy folyamat megbízhatósága az érettségi szintjével egyenes arányú összefüggésben van, a bizalom kialakítása és fenntartása alapvetően a validált bizalmi modellre épül.

A szervezetek megbízhatósága

Az egyes szervezetek mindinkább kapcsolati függőségben találják magukat a gazdaság, az informatika és a biztonság területén egyaránt. A külső kapcsolatok egyrészről működésbeli és költségbeli hatásfok-javulást okozhatnak, másrészről a függőségek megléte újabb vagy épp a meglévő kockázatokra vonatkozóan magasabb kockázati szintet jelenthetnek.

Ahogy a kockázat, úgy a bizalom mértéke sem csak a két véglet értékét veheti fel (teljes értékű vagy nem létező), hanem a két végérték által definiált intervallum bármelyik értékét. Ezen felül a bizalmi szint időben is változhat, minthogy az azt befolyásoló tényezők (pl. kockázati étvágy, üzleti cél, új bizonyíték stb.) változása szintén kihatással lehet a bizalmi kapcsolatra, kapcsolatokra.

A szervezeti szintű megbízhatóság a szervezet által használt vagy alkalmazott erőforrások bizalmi szintje alapján határozható meg. E megállapítás kiváltképp nagy jelentőséggel bír a folyamatok terén. Az adott szervezet képességeinek, ezáltal megbízhatóságának alátámasztása a releváns folyamatok megfelelőségének bizonyításával lehetséges, például egy nemzetközi vagy iparági szabvány ellenében történő tanúsítás elérésével és fenntartásával. Az információbiztonság területén a megbízhatóságot az ISO/IEC 27001:2013[24] vagy más iparági szabványok (pl. Payment Card Industry Data Security Standard) szerinti tanúsítás elérése jelenti. A szabványok ellenében történő tanúsítás a közvetített bizalmi modellt valósítja meg.

A továbbiakban példaként a kötelező jellegű bizalmi modellt megvalósító néhány jelentősebb magyarországi, illetve uniós jogszabályi előírást ismertetek:

- Az elektronikus információbiztonság tekintetében *az állami és önkormányzati szervek elektronikus információbiztonságáról* szóló 2013. évi L. törvény felhatalmazása alapján a Nemzeti Elektronikus Információbiztonsági Hatóság

[24] ISO/IEC 27001:2013. Information technology - Security Techniques - Information security management systems — Requirements, International Organization for Standardization, 2013.

(NEIH) működését az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint *az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról* szóló 187/2015. (VII. 13.) Korm. rendelet, míg a Kormányzati eseménykezelő központ működését *a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól* szóló 185/2015. (VII. 13.) Korm. rendelet szabályozza.

- A pénzügyi szolgáltatást végző gazdasági társaságok számára felügyeleti szervként *a hitelintézetekről és a pénzügyi vállalkozásokról* szóló 2013. évi CCXXXVII. törvény a Magyar Nemzeti Bankot (MNB) teszi meg.
- Az adatvédelem tekintetében *az információs önrendelkezési jogról és az információszabadságról* szóló 2011. évi CXII. törvény a Nemzeti Adatvédelmi és Információszabadság Hatóságot (NAIH) autonóm államigazgatási szervként jelöli ki.
- *Az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról* szóló Európai Parlament és a Tanács 460/2004/EK rendelete hozta létre az ENISA[25] szervezetét. Az Ügynökség működését, hatókörét *az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről* szóló Európai Parlament és a Tanács 526/2013/EU rendelete módosította 2013-ban. Az ENISA feladatköre együttműködni a tagállamokkal és különböző gazdasági társaságokkal, tanácsadás, gyakorlatok szervezése, a CSIRT-ek (Computer Security Incident Response Teams) együttműködésének elősegítése stb.
- *A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről* szóló Európai Parlament és a Tanács (EU) 2016/1148 irányelve, úgynevezett NIS irányelv „*az első közösségi szintű szabályozás az információbiztonság területén, mely kötelezően és geopolitikai alapon határoz meg szabályokat és kötelező együttműködést egyes intézmények számára*”[26], mely az érintett szervezetek közötti bizalom szintjének növelését hivatott elősegíteni.

Az informatikai rendszerek megbízhatósága

Az informatikai eszközök és szolgáltatások megbízhatóságát erősen befolyásolja a kialakításukban felhasznált építőelemek, alkalmazott módszertanok, folyamatok, valamint a közreműködő szakemberek jellege és tudása. Az operatív folyamatok működtetésében is ugyanezen tényezők jelennek meg. Az építkezés már az alkatrészek szintjén megkezdődik, minthogy példának okáért az adott CPU[27] utasításkészlet, elágazásbecslés stb. megvalósításának helyessége alapvető fontosságú. Egy magasabb absztrakciós szinten egy informatikai céleszköz (router, tűzfal stb.) vagy általános jellegű eszköz (szerver, munkaállomás stb.) az építőelem,

[25] ENISA (European Union Agency for Network and Information Security – Európai Uniós Hálózat- és Információbiztonsági Ügynökség)

[26] KORMÁNYZATI ESEMÉNYKEZELŐ KÖZPONT: Megjelent a hálózati és információs rendszerek biztonságáról szóló EU-s irányelv, http://www.cert-hungary.hu/nis_directive (Letöltés ideje: 2018. 10. 16.).

[27] CPU (Central Processing Unit – Központi számítóegység)

ezt követően a belőlük épített rendszer és az arra építő szolgáltatás összessége jelenik meg.

A funkcionalitás az egyes elemek együttes helyes működéséből, míg a biztonsági funkcionalitás a megfelelő információbiztonsági kontrollok megfelelő alkalmazásából fakad. A szervezetre szabottan a megfelelő kontrollok kiválasztásában a kockázatmenedzsment megvalósítása jelenti a megoldást.

A NIST SP800-53 alapján a biztonsági funkcionalitás (Security functionality) a biztonsági szabályozásban lefektetett biztonsági cél vagy célok adott informatikai alkatrész, eszköz, rendszer stb. általi megvalósítása, implementálása, amellyel biztosítható, hogy a lehetséges kockázatok a bizalmasság, a sértetlenség és a rendelkezésre állás vonatkozásában az elfogadható kockázati tartományban legyenek[28].

A biztonsági funkcionalitás szavatolása kritikus fontosságú egy informatikai rendszer megbízhatóságának megítélésében. A biztonsági funkció kritikus része az adott informatikai rendszer létrehozása (tervezése és megalkotása), valamint az állapot fenntartásának folyamata, ahol a létrehozás a rendszer építését, akvizícióját és szoftverfejlesztését is jelentheti. A másik fontos tényező a belső és/vagy külső fél által folytatott audittevékenység, amely ellenőrzi a biztonsági funkcionalitásnak való megfelelőséget az életciklus minden egyes szakaszára vonatkozóan. Az audittevékenységek közé tartozik például a penetrációs teszt végrehajtása és a kapcsolódó folyamatok vizsgálata.

A NIST SP800-53 alapján a biztonsági funkcionalitás szavatolása (Security assurance) egy informatikai alkatrész, eszköz, rendszer stb. felé irányuló bizalom mértéke abban a tekintetben, hogy az elvárt biztonsági funkcionalitást megvalósítja[29].

A fentiekből következik, hogy a biztonsági funkcionalitás és a megbízhatósági paraméter szoros kapcsolatban áll egymással. A rendszer létrehozásakor a tervezők, fejlesztők, implementálók bizonyítékkal szolgálnak, melyet validációs és verifikációs tesztek során értékelnek. A bizonyíték lehet szoftver- és/vagy rendszer-architektúra, forráskód biztonsági átvilágításának eredménye, különböző dokumentációk eredménye stb.

Az informatikai eszközök működésük során számos állapotváltozáson mennek keresztül, ugyanakkor megbízhatóságukat minden állapot esetében szavatolni kell. Az aktuális állapot csak akkor tekinthető biztonságosnak, ha abba egy megbízható kiinduló állapotból biztonságos állapotokon keresztül jutott el az adott rendszer. Azonban már egy olyan egyszerűnek tűnő feladat, mint egy rendszerindítás, hatalmas buktatókat tartogathat.

---

[28] NIST: Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, p. 21. (Letöltés ideje: 2016. 03. 02.)

[29] NIST: Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, p. 21. (Letöltés ideje: 2016. 03. 02.)

E problémakört a TCG[30] szervezet Trusted Computing koncepciója hivatott orvosolni, mely az informatikai eszközök működésének, informatikai rendszerek és szolgáltatások elérhetőségének megbízható, számon kérhető, szabályozható, fenntartható és biztonságos, továbbá minden állapotra kiterjedő megvalósítása.

A definíció szerinti általános Trusted Computing funkciók a következők[31]:

- Biztonságos indulás (Secure boot) által az adott informatikai eszköz az indulási folyamat során a definiált biztonságos és megbízható konfigurációval jusson el a felhasználó által már használható, szintén biztonságos állapotba.
- Szeparált memória (Curtained memory) a memória elkülönítését jelenti abból a célból, hogy más felhasználói, rendszerszintű vagy hibakereső (debugger) folyamatok ne férjenek hozzá az adott folyamat memóriájához olvasás szintjén sem.
- Titkosított tároló (Sealed storage) által biztosított, hogy az adatvagyon kriptográfiai módszertanok alkalmazásával biztonságosan kerüljön tárolásra.
- Biztonságos I/O (Secure I/O) által meggátolható az I/O eszközök működésének megfigyelése (pl. billentyűzet bevitele) vagy manipulálása (pl. kijelzőre küldött adatok módosítása).
- Sértetlenség biztosítása (Integrity measurement) a futtatható kódokra vonatkozó kivonatkészítés (hashing) által.
- Távoli hitelesítés (Remote attestation) tulajdonképp az adott rendszer megbízhatóságát jelenti a kommunikációban részt vevő más rendszerek számára.

A TCG beágyazott rendszerek, tároló, hálózati, mobil eszközök, IoT (Internet of Things), továbbá felhőszolgáltatás és virtualizált rendszerek esetén nyújt megoldást. A TCG által specifikált TPM[32] modul[33] a következő képességekkel bír[34]:

- Nyilvános kulcs alapú titkosítás,
- Hashing funkció,
- Kulcs létrehozása és kezelése,
- Biztonságos tárolás a kulcsok és egyéb érzékeny adatok számára,
- Véletlenszám-generálás,
- Sértetlenség biztosítása,
- Hitelesítés.

Az UEFI[35] a biztonságos indítás megvalósítására nyújt megoldást[36], amely a TPM chippel együttműködve a megbízhatóság szintjét emeli[37].

---

30 Trusted Computing Group

31 J. Christopher BARE: Attestation and Trusted Computing, https://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/bare.pdf (Letöltés ideje: 2016. 03. 20.)

32 Trusted Platform Module

33 ISO/IEC 11889-1:2015. Information technology – Trusted platform module library, International Organization for Standardization, 2015.

34 BARE i. m., p. 2.

35 Unified Extensible Firmware Interface

36 UNIFIED EFI, INC.: Unified Extensible Firmware Interface Specification, http://www.uefi.org/sites/default/files/resources/UEFI%20Spec%202_6.pdf (Letöltés ideje: 2016. 03. 02.)

E megoldások azonban a biztonság és ezzel a bizalmi szint növelésének lehetőségét biztosítják, azonban nem szavatolják annak (megfelelő) alkalmazását.

Az informatikai eszközökre vonatkozó külső szervezet általi független értékelés meghatározó szabványa az Információs technológia biztonsági értékelésének közös kritérium, azaz Common Criteria for Information Technology Security Evaluation, melyet az ISO/IEC 15408[38] szabványban definiál. A Common Criteria lehetőséget biztosít biztonsági funkcionalitás specifikálásához és a specifikálás ellenében a meglévő és egyben reprodukálható bizonyítékok alapján történő megfelelésének.

A Common Criteria felépítése a biztonsági funkcionalitás meghatározására, valamint annak ellenében való értékelésére és szavatolására tagozódik[39]:

- TOE[40] a minősítési folyamat tárgyát képező informatikai megoldást definiálja. A tanúsítási eljárás tárgyát szoftver, firmware vagy hardvereszköz is képezheti, ugyanakkor egy teljes informatikai termék vagy annak egy részegysége, vagy informatikai termékek együttműködő egysége is vizsgálható és minősíthető.
- PP[41] az általános igényeket és felhasználói célokat tartalmazza, amelyet a minősítési folyamat során egy TOE részéről teljesíteni szükséges. A problémát, a problémakört, illetve a kapcsolódó elvárásokat a végfelhasználók specifikálják. A gyártói megoldások esetében egy vagy egyszerre több PP ellenében történő megfelelés is lehetséges és kivitelezhető megoldás.
- ST[42] olyan leírás, amely a minősítési folyamat alá helyezett TOE esetében a kitűzött célokat és igényeket, valamint a megvalósítandó funkcionalitást és annak biztosítási, szavatolási módját tartalmazza. A profillal ellentétben egy ST termékspecifikus meghatározásokat tartalmaz.
- SFRs[43] azoknak a biztonsági funkcióknak a halmaza, amelyeket egy adott TOE teljesítheti. A funkcionális követelmények osztályokba sorolhatók, melyeket családok és azok összetevői alkotnak. Egy SFR egy vagy több előírásgyűjteményt definiálhat Biztonsági funkciók szabályzatában (SFP[44]) a vonatkozó célok, erőforrások, információk és eljárások meghatározása végett[45].

---

37 Tom OLZAK: UEFI and the TPM: Building a foundation for platform trust, http://resources.infosecinstitute.com/uefi-and-tpm/ (Letöltés ideje: 2016. 03. 10.)

38 ISO/IEC 15408:2009. Information technology – Security techniques – Evaluation criteria for IT security, International Organization for Standardization, 2009.

39 COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (Letöltés ideje: 2016. 03. 02.)

40 TOE (Target Of Evaluation – Értékelés tárgya)

41 PP (Protection Profile – Védelmi profil)

42 ST (Security Target – Biztonsági előirányzat)

43 SFRs (Security Functional Requirements – Biztonsági funkcionalitás követelményei)

44 SFP (Security Functional Policy – Biztonsági funkciók szabályzata)

45 COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf, p. 18. (Letöltés ideje: 2016. 03. 11.)

Fontos kiemelni, hogy a funkcionális függőségek következtében egy adott SFR teljesítése további funkciók megvalósítását követelheti meg. Továbbá a Common Criteria nem teszi kötelezővé egy-egy funkció Biztonsági előirányzat dokumentumban való feltüntetését.

A Common Criteria v3.1R4 által definiált osztályok[46]:

- FAU: Biztonsági átvilágítás (Security audit),
- FCO: Kommunikáció (Communication),
- FCS: Kriptográfiai támogatás (Cryptographic support),
- FDP: Felhasználói adatvédelem (User data protection),
- FIA: Azonosítás és hitelesítés (Identification and authentication),
- FMT: Biztonsági irányítás (Security management),
- FPR: Titoktartás (Privacy),
- FPT: A TSF védelme (Protection of the TSF),
- FRU: Erőforrás-felhasználás (Resource utilisation),
- FTA: TOE-hozzáférés (TOE access),
- FTP: Bizalmi útvonal/csatornák (Trusted path/channels).

A Biztonsági funkcionalitás szavatolása (SARs[47]) biztonsági funkciók értékelésének, a megbízhatóság szavatolásának módját definiálja, amely egy adott TOE által teljesítendő. A Common Criteria v3.1R4 által definiált osztályok[48]:

- APE: A védelmi profil értékelése (Protection profile evaluation),
- ASE: A biztonsági előirányzat értékelése (Security target evaluation),
- ADV: Fejlesztés (Development),
- AGD: Az útmutató dokumentumok (Guidance documents),
- ALC: Az életciklus támogatása (Life-cycle support),
- ATE: Vizsgálatok (Tests),
- AVA: A sebezhetőség felmérése (Vulnerability assessment),
- ACO: Összeállítás (Composition).

Az értékelési folyamat során a védelmi profilt, a biztonsági előirányzatot és az értékelés tárgyát kell megítélni, mely folyamatok során az eredmények bekerülnek a megfelelő nyilvántartásba. Az egyszerű TOE-komponensek értékelésekor értékelési garancia szint (EAL[49] szint), míg komplex TOE esetén összetett garancia csomagok (CAP[50] szint) kerülnek meghatározásra. Az értékelési garanciaszintek az alábbiak[51]:

---

[46] COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf, pp. 29-42. (Letöltés ideje: 2016. 03. 11)

[47] SARs (Security Assurance Requirements – Biztonsági funkcionalitás szavatolása)

[48] COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf (Letöltés ideje: 2016. 03. 11.).

[49] EAL (Evaluation Assurance Level – Értékelési garancia szint)

[50] CAP (Composed Assurance Package – Összetett garancia csomag)

- EAL 1: Funkcionálisan vizsgált (Functionally tested),
- EAL 2: Strukturálisan vizsgált (Structurally tested),
- EAL 3: Módszeresen vizsgált és ellenőrzött (Methodically tested and checks),
- EAL 4: Módszeresen tervezett, vizsgált, és átnézett (Methodically designed, tested and reviewed),
- EAL 5: Félformálisan tervezett és vizsgált (Semiformally designed and tested),
- EAL 6: Félformálisan igazolt tervezésű és vizsgált (Semiformally verified design and tested),
- EAL 7: Formálisan igazolt tervezésű és vizsgált (Formally verified design and tested).

A komponens szavatolási csomagok az alábbiak[52]:

- CAP-A: Strukturálisan összeállított (Structurally composed),
- CAP-B: Módszeresen összeállított (Methodically composed),
- CAP-C: Módszeresen összeállított, vizsgált és átnézett (Methodically composed, tested and reviewed).

Az ISO/IEC 15408:2009 szabvány ellenében megvalósított tanúsítás a közvetített bizalmi modellt valósítja meg.

Összefoglalás, következtetések levonása

Egy szervezet, szervezeti egység, egyén, a folyamatok, valamint az alkalmazott technikai eszközök felé irányuló bizalom mértéke összefüggésben van az önnön megbízhatósági paraméterével. Megállapítható, hogy a bizalom kialakítása az ISACA BMIS modell négy alapelemére, azaz az ember, a folyamat, a szervezet és a technológia vonatkozásában egyaránt értelmezhető, továbbá az egyes elemek felé történő bizalmi szint kialakításában alkalmazott megközelítés a NIST által kialakított bizalmi modellek egyikének megfeleltethető.

A bizalmi modellek közé a validált bizalmi modell (Validated trust), a közvetlen történeti bizalmi modell (Direct historical trust), a közvetített bizalmi modell (Mediated trust), kötelező bizalmi modell (Mandated trust), valamint a hibrid bizalmi modell (Hybrid trust) tartozik. Az egyes modellek között jóság szerinti sorrend nem alkotható meg, ahogy a különböző szervezetek, szervezeti egységek, különböző folyamatok, a technikai megoldások más-más megközelítést igényelnek.

A tárgyaltak értelmében az Európai Unió számára védelmi képességeire vonatkozó hatékonyságnövelés érdekében kialakítandó és folyamatosan fejlesztésre

---

[51] COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf, pp. 30-45. (Letöltés ideje: 2016. 03. 11.)

[52] COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf, pp. 46-53. (Letöltés ideje: 2016. 03. 11.)

szoruló együttműködés megvalósítására a BMIS négy alapelemét figyelembe kell venni az alkalmazott bizalmi modell jellegétől függetlenül. A biztonságra vonatkozó meghatározó axióma, miszerint a biztonság szintjét mindig a „leggyengébb láncszem" határozza meg, a tárgyalt négy alapelem vonatkozásában együttesen, egy rendszerként szükséges tekinteni.

Felhasznált irodalom:

- Annegret BENDIEK: European Cyber Security Policy, SWP Research Paper, 2012.
- AZ UNIÓ KÜLÜGYI ÉS BIZTONSÁGPOLITIKAI FŐKÉPVISELŐJE: KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése, Brüsszel: EURÓPAI BIZOTTSÁG, 2017.
- BEDERNA Zsolt: Az Általános adatvédelmi rendelet és az információbiztonság kapcsolódási pontjai, Szakmai Szemle, 2018/ 3., pp. 76-103.
- COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (Letöltés ideje: 2016. 03. 02.)
- COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf (Letöltés ideje: 2016. 03. 11.)
- COMMON CRITERIA RECOGNITION ARRANGEMENT (CCRA): Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf (Letöltés ideje: 2016. 03. 11.)
- ISACA: COBIT 5, 2012.
- ISACA: Process Assessment Model (PAM): Using COBIT 5, 2013.
- ISACA: The Business Model for Information Security, ISACA, 2010.
- ISO/IEC 11889-1:2015. Information technology – Trusted platform module library, International Organization for Standardization, 2015.
- ISO/IEC 15408:2009. Information technology – Security techniques – Evaluation criteria for IT security, International Organization for Standardization, 2009.
- ISO/IEC 15504:2013. Information technology – Process assessment, International Organization for Standardization, 2013.

- ISO/IEC 27001:2013. Information technology – Security Techniques – Information security management systems — Requirements, International Organization for Standardization, 2013.
- ISO/IEC 33001 Information technology – Process assessment – Concepts and terminology, International Organization for Standardization, 2015.
- ISO/IEC 9001:2015, International Organization for Standardization, 2015.
- ISO/IEC/IEEE 15288:2015 Systems and Software Engineering, International Organization for Standardization, 2015.
- J. Christopher BARE: Attestation and Trusted Computing, https://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/bare.pdf (Letöltés ideje: 2016. 03. 20.)
- KORMÁNYZATI ESEMÉNYKEZELŐ KÖZPONT: Megjelent a hálózati és információs rendszerek biztonságáról szóló EU-s irányelv, http://www.cert-hungary.hu/nis_directive (Letöltés ideje: 2018. 10. 16.)
- Lance SPITZNER: Defining the Security Awareness Maturity Model, https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model (Letöltés ideje: 2018. 05. 09.)
- NIST: Managing Information Security Risk, https://doi.org/10.6028/NIST.SP.800-39 (Letöltés ideje: 2016. 03. 05)
- NIST: Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Letöltés ideje: 2016. 03. 02.)
- PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1549211879330 (Letöltés ideje: 2019. 02. 03.).
- Tom OLZAK: UEFI and the TPM: Building a foundation for platform trust, http://resources.infosecinstitute.com/uefi-and-tpm/ (Letöltés ideje: 2016. 03. 10.)
- UNIFIED EFI, INC.: Unified Extensible Firmware Interface Specification, http://www.uefi.org/sites/default/files/resources/UEFI%20Spec%202_6.pdf (Letöltés ideje: 2016. 03. 02.)

Felhasznált jogszabályok:

- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági

felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

- 1995. évi CXXV. tv. a nemzetbiztonsági szolgálatokról
- 2009. évi CLV. tv. a minősített adat védelméről
- 2011. évi CXII. tv. az információs önrendelkezési jogról és az információszabadságról
- 2012. évi I. tv. munka törvénykönyve
- 2013. évi CCXXXVII. tv. a hitelintézetekről és a pénzügyi vállalkozásokról
- 2013. évi L. tv. az állami és önkormányzati szervek elektronikus információbiztonságáról
- Európai Parlament és a Tanács (EU) 2016/1148 irányelve (a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről)
- Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- Európai Parlament és a Tanács 460/2004/EK rendelete (az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról)
- Európai Parlament és a Tanács 526/2013/EU rendelete (az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről)

HASILLÓ GYÖRGY

BEMUTATKOZIK A GÁZOLÁSOS TERRORCSELEKMÉNYT MEGAKADÁLYOZÓ VÉDELMI RENDSZER

I. Bevezetés

Napjaink egyik legveszélyesebb terrorfenyegetése a gépjárművel történő gázolásos terrorcselekmény, amely a támadás olyan formája, aminek során az elkövető szándékosan gépjárművel hajt a célpontnak azzal a céllal, hogy a lehető legkomolyabb sérülést, vagy a lehető legnagyobb vagyoni kárt okozza.[1]

Az ilyen jellegű akciókat rendszerint könnyű célpontok ellen követik el – úgymint járókelők, rendezvények résztvevői, nagyobb csoportosulások –, tehát gyakorlatilag szinte mindig olyan emberek, akik többedmagukkal vannak jelen nyilvános helyen, ahol tevékenységük közben nem számítanak ellenük irányuló terrorcselekményre.

Ismereteink szerint 2014 óta összesen 17 esetben követtek el terroristák gázolásos cselekményt a világon, melyek összesen 173 halálos áldozatot és 667 sérülést okoztak.[2]

Az eddigi legpusztítóbb európai támadás a 2016. július 14-i nizzai merénylet volt: a francia nemzeti ünnep miatt zsúfolt esti, tengerparti sétányon több száz méteren keresztül tudott nagy sebességgel végighajtani a merénylő által vezetett teherautó, összesen 86 ember halálát és 434 ember sebesülését okozva.[3]

Az efféle cselekmények magas száma azt mutatja, hogy ez a támadási forma a terroristák egyik kedvelt eszközévé vált, viszonylag olcsó, könnyen kivitelezhető, akár egy személy által is megvalósítható, pusztítása pedig félelmetes. A témával tehát szükséges és időszerű foglalkozni.

Amint arra Rácz András és Brestyánszki Flóra elemzése is kitér: *„A ramminghez nincs szükség sem különösebb felkészülésre, kiképzésre, sem speciális szakértelemre: kis túlzással mindössze vezetési tudás és egy alkalmas jármű kell hozzá…Egy ramming támadás előkészítésére akár néhány óra is elegendő lehet, már az autóbérlést is beleszámítva.”*[4]

---

1 Transportation Security Administration Office of Security Policy and Industry Engagement Surface Divison - Highway and Motor Carrier Section: Vehicle Ramming Attacks Threat Landscape, Indicators, and Countermeasures May 2017. https://publicintelligence.net/tsa-vehicle-ramming/ (Letöltés ideje: 2017. 12. 05.)

2 Transportation Security Administration: i. m. 1.

3 RÁCZ András – BRESTYÁNSZKI Flóra: A gépjárművel végrehajtott, ramming típusú terrortámadásokról és a védekezés lehetőségeiről. http://archiv.netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-14-a-gepjarmuvel-vegrehajtott-ramming-tamadasokrol-racz-a-brestyanszki-f.original.pdf (Letöltés ideje: 2017. 12. 01.)

4 Uo.

Jelen írásom egy olyan komplex rendszer elméletét vázolja fel, amely kifejezetten az ilyen támadások megakadályozására készülhetne el. A dokumentum kizárólag elméleti síkon vázolja a rendszer bemutatását, annak elemeit, működését. A ma rendelkezésre álló technológiák, illetve a mérnöki tudomány aktuális állása alapján a rendszer kivitelezhető a megfelelő tervezést követően.

Célom, hogy még ha csak elméleti szinten is, de segítséget nyújtsak a rendvédelmi szervek jövőbeli tevékenységéhez, az aljas, gonosz szándékból elkövetett merényletek megakadályozásában, melyek ártatlan emberéleteket veszélyeztetnek szerte a világon.

A rövid bevezetés után bemutatom a rendszer elemeit, működési elvét, illetve két példán keresztül ismertetem hatékonyságát.

II. Bemutatkozik a GTMVR

A *gázolásos terrorcselekményt megakadályozó védelmi rendszer* (GTMVR) egy olyan komplex szisztéma, amely a közterületek autóktól elválasztott területeit hivatott megvédeni a gépjárműves támadásokkal szemben. Öt fő komponensét alkotják a járdákba épített rejtett, avagy süllyesztett oszlopok, az ezeket és a különböző szenzorokat is vezérlő mesterséges intelligencia (a továbbiakban: MI), a támadó személyek ellen fellépő drónok, az egész rendszer mögött álló, folyamatosan bővülő adatbázis, valamint a kisegítő eszközök, úgymint kamerák, érzékelők, internethálózat.

Ahhoz, hogy a teljes rendszer működési elvét megértsük, szükséges egyenként végigtekinteni az egyes elemeken.

1. Oszlopok

Az oszlopok a járdaszegélyekbe és a járdákba épített süllyesztett, nagy teherbírású jármű behatolásgátló elemek. Ezek mindaddig rejtve maradnak, amíg a támadás be nem következik, ezáltal nem zavarják a járda forgalmát, valamint esztétikai szempontból sem rombolják a környezetet. Egyetlen feladatuk van, megakadályozni a járdára felhajtó támadó jármű továbbhaladását, illetve megállítás után a helyszín elhagyását.

2. Mesterséges intelligencia

A vezérlő MI egy olyan tanulásra képes szoftver, amely a rendelkezésére álló szenzorok, kamerák, érzékelők és a mögötte álló adatbázis által felállított mintázatok alapján képes reagálni az adott terrorcselekményre, úgy, hogy a támadás bekövetkezésekor megpróbálja izolálni a támadási területet, és az általa meghatározott pontokon felemeli a mindaddig rejtett oszlopokat, megakadályozva ezzel a jármű továbbhaladását. Mindig csak azok az elemek emelkednek ki, amelyek a legközelebbi lehetséges megállítási ponton sorakoznak, illetve a program számításai alapján a megállítási esélyt növelhetik. Tehát lehetséges olyan oszlop-kiemelkedés is, ami már a jármű alatt van, de felemelkedésével segédkezhet a jármű megállításában. Továbbá a jármű visszafelé haladását is meggátolják az oszlopok,

így a támadó nem tudja elhagyni a helyszínt, nem tud újabb támadási zónát keresni, és ezáltal még több embert veszélybe sodorni.

3. Drónok

A drónok kis méretű, változtatható fegyverzettel felszerelt, pilóta nélküli robotrepülőgépek, elsődleges feladatuk a támadó jármű személyzetének kiiktatása, amennyiben azok a megállítás után továbbra is harcképesek maradnak. A kiszálló terrorista személyeket a drónok körbeveszik és kiiktatják. A kiiktatás módja lehet a sokkoló használata, de a drónok kiiktathatják akár a kézben tartott lőfegyvereket is. A védekezés mértéke szabadon állítható, bizonyos szintig az MI-re bízható. A lényeg, hogy ezek hatására a támadó nem képes további cselekményekre és a jármű mellett marad a hatósági intézkedésig.

4. Adatbázis

Az adatbázis az MI tudását bővíti már megtörtént esetek adatainak tárolásával, mely alapján a program képes létrehozni egy „képet" arról, hogy mit jelent egy ilyen gázolásos terrorcselekmény. Képes a korábbi esetek alapján egyfajta mintázatot létrehozni az elkövetők és járműveik fajtáiról, sebességükről, a járművek műszaki adatairól, tehát gyakorlatilag minden információnak rendelkezésre kell állnia a korábbi esetekről, hogy azokat a program elemezni tudja és későbbi terrorcselekmények megakadályozásához fel tudja használni. Röviden összefoglalva, az a cél, hogy a program minden eseményt követően tanuljon, fejlődjön, okosodjon.

5. Kisegítő eszközök

Kisegítő eszközök összefoglaló névvel illetem mindazokat a kamerákat, szenzorokat, hálózati elemeket és egyéb felszereléseket, amelyek a rendszer szemei és fülei lesznek. Ezen eszközök nélkül a rendszer képtelen lenne működni.

A felsorolás és a rövid bemutatás után egyenként, részletesen tekintjük át az egyes elemeket és azok tulajdonságait.

III. A GTMVR elemeinek részletes jellemzése

1. Oszlopok

Az oszlopok jelentik a GTMVR pajzsát, ezek az eszközök azok, amelyek útját állják akár a többtonnás járműveknek is. A kereskedelemben kapható modellek közül a TISO AUIA-348 (M30) típusú oszlop fizikai adottságaiból indultam ki, mert ezek a célnak megfelelőek lehetnek. A típus meghatározása nem jelenti azt, hogy konkrétan ezzel az eszközzel működne a végleges rendszer, annak csupán az adatait használom szemléltetésre. A nyugvó állapotában földbe csúsztatott 1000 mm magas elem 600 mm mélyen van installálva. Átmérője 325 mm. Energiaelnyelő képessége 1845,8 kJ.

A ramming típusú támadásokat nagyrészt személyautókkal követik el, de előfordult már teherautóval, kamionnal történő gázolás is, emlékezzünk csak a nizzai tragédiára. Egy rövid számolás során próbáljuk meg a legnehezebb és legnagyobb járművet kiválasztani. A kérdés tehát az, hogy milyen sebességgel mozoghat az adott tárgy – jelen esetben egy 40 tonnás kamion –, hogy az oszlop még elnyelje a mozgási energiáját, gyakorlatilag 0 távolságon belül úgy, hogy az oszlop még nem sérül.

A kamion mozgási energiája E=1/2*m*v2=1/2*40 000 kg*v2 (m=40 000 kg) W=1845 kJ azaz más mértékegységgel W=1845 000 kg*m2/s2
Az egyszerűség kedvéért feltételezzük, hogy E=W, és hagyjuk el az integrálszámítást, a tárgy az adott sebességről rövid időintervallum alatt lassul zérus sebességre, ezzel maximális lassulást elérve, valamint feltételezzük, hogy az összes mozgási energiát az oszlop nyeli el, eltekintve a tárgy ütközési deformációjától.
Így v kifejezve:
v=√((2)*"E/m)"
azaz: v=√((2)*1845000/40000) = 9,6 m/s ami v=34,4 km/h, ami nem biztos, hogy elegendő, ha a kamion 50-60 km/h sebességgel érkezik.

Ugyanez a számítás személygépkocsi esetén (m=1000 kg).
v=√((2)*1845000/1000) =60,7 m/s=218,6 km/h, tehát ha a támadó személygépkocsit használ, akkor az oszlop lényegesen gyorsabban érkező autót is képes megállítani.

A szemléltetés célja az volt, hogy kiindulópontot adjon az oszlop tulajdonságait illetően; látható, hogy a végleges rendszerhez ismerni kell az eszköz minden tulajdonságát, pontos számításokra van szükség és természetesen lényeges az adott területen történő elhelyezkedés is.

A rendszer tervezésekor az első lépések egyikének kell lennie a védett területek meghatározásának, amikoris figyelembe kell venni minden lehetséges tényezőt, például azt, hogy milyen sűrűn kerüljenek elhelyezésre az oszlopok, milyen látogatottságú útvonalnál helyezkednek el, az úttest és a járda viszonya, például a járda magassága, kerékpárút megléte vagy a forgalmi rend.

A GTMVR változtatható felépítésű kell hogy legyen, hogy a különféle védett zónákhoz még inkább alkalmazkodni tudjon. Nem egyforma sűrűségű oszlopkihelyezés szükséges egy szűkebb utca elé, mint amilyen például egy nagyobb nyílt tér köré szükséges. Meg kell vizsgálni, hogy az adott helyen milyen csatornázás van, milyen földkábelek futnak az úttest alatt, ezeket mind számításba kell venni az egyes elemek elhelyezésekor. Nagyon fontos a teherbírás, hogy egy adott oszlop milyen sebesség mellett képes megállítani a támadó járművet, ugyanakkor az anyagminőség, az esetleges javítások mértéke, ára is szerepet játszhat a megfelelő eszköz kialakításában, gyártásában. Részletkérdésnek tűnik, ám ugyanolyan fontos a zárófedél meghatározása, lesz-e ilyen az oszlop felett, vagy magának az eszköznek van valamilyen víz- és ütésálló felsőrész kialakítása.

2. Drónok

A drónok használatának célja a megállított járműből kiszálló célszemély semlegesítése, mielőtt az bárminemű további cselekményt el tudna követni. A

kereskedelemben kapható kis méretű drónok közül a DJI Spark elnevezésű termék fizikai adottságaiból indultam ki, méretében ez lenne megfelelő a maga 14,3 x 14,3 x 5,5 cm-es testével. Négy rotoros kialakításának előnye a stabilitás mellett a ki- és behajtható propellerek, kiváló aerodinamikai teljesítménye, valamint sebessége, ami pedig elérheti az 50 km/h-t is. A rendszerbe integráláshoz természetesen további intelligens tényezők szükségesek, ám már a Spark kereskedelmi kivitelezése is képes gesztusok felismerésére, valamint önálló hazatérésre. Nem kizárólag a mérete miatt választottam, de a célnak a kereskedelemben kapható típus nem lenne megfelelő, hiszen számos hiányossággal küzd, például ez az eszköz nem használható esőben, illetve a teherbírása is kérdéses. A mérete viszont indikatív.

A védett területeken belül adott távolságonként rejtve, kettesével kerülnek elhelyezésre és tárolásra ezek a drónok, melyeket a mesterséges intelligencia aktivál támadás esetén. Ekkor a teljesen önállóan repülni képes eszközök megközelítik a járművet, illetve az abból kiszálló célszemélyt, felszólítják a megadásra és utasítják, hogy feküdjön a földre. Természetesen a beprogramozható szövegek, hangjelzések, mind változtathatók. Amennyiben a személy követi az utasításokat, a drónok felügyelet alatt tartják a rendvédelmi szervek érkezéséig. Ha a célszemély nem követi az utasításokat és megpróbálja elhagyni a helyszínt, vagy támadásra készül akár a drónok, akár a közelben lévő civilek vagy rendőri erők ellen, a drónok (a betáplált programnak megfelelően) hatástalanítják a célszemélyt. A mesterséges intelligencia feladata meghatározni a fellépés mértékét, például amennyiben a célszemély fegyvertelenül, sebesülten próbál elfutni, elegendő, ha a drónok sokkolóval kényszerítik maradásra. A kényszerítő eszközök típusairól és azok használatáról írásom nem ad részletes leírást, azt a megfelelő jogszabályok keretein belül célszerű rendezni.

Gondoskodni kell a drónok tárolásáról a védelmi eszközök közelében; pontos számításokat igényel az eszközök helyszínre érkezési ideje, hiszen a támadás bekövetkezése után mielőbb meg kell közelíteniük a gyanúsítottat. A drónok tárolóhelye (a továbbiakban: drónrekesz) gondosan megtervezett, szeparált, időjárási viszonyoknak ellenálló, az eszközök akkumulátorának töltését biztosító berendezés kell hogy legyen. A drónrekesz legyen képes zárt láncú kommunikációra az MI-vel és a parancsnoksággal. A kapcsolat célja egyrészt a vezérlés, másrészt a különböző adatok kinyerése, mint az akkumulátor töltöttség, fegyverzet állapota, karbantartás szükségessége.

3. Mesterséges Intelligencia

Mi a mesterséges intelligencia? A mesterséges intelligencia nem más, mint olyan feladatok megoldása számítógéppel, amelyek emberi intelligenciát igényelnek. Az intelligencia az elme elemző és megkülönböztető képessége. Mentális képesség: egy új szituációhoz való gyors és sikeres alkalmazkodás, a következtetés használatának képessége a problémamegoldásban.[5] Az MI lesz a rendszer agya. Egy olyan innovatív szoftverről van szó, amely a megfelelő rutinok és protokollok figyelembevételével összesíteni tudja a beérkező adatokat – legyen szó akár a kamerák képeiről, akár a sebességmérő szenzorokról – és azokat

[5] Merriam Webster Dicitionary: Intelligence. https://www.merriam-webster.com/dictionary/intelligence (Letöltés ideje: 2018. 01. 02.)

kielemezve döntéseket képes meghozni a rendelkezésre álló eszközök felhasználásával. Az MI egyik alapvető tulajdonsága a tanulás képessége, a szoftver ugyanis az indulás előtt betáplált adatok után a folyamatosan beérkező információk által okosodik, ráadásul a nem közvetlenül a GTMVR-ba beérkező adatokat is fogadni tudja a háttéradatbázis segítségével. Így nem csupán a rendszer által felfogott adatokból tanulhat, hanem a világ más részein történő események után is, amennyiben azok információi rögzítésre kerülnek az adatbázisba. Az MI képes ezeket az adatokat rendszerezni, ezekből kockázatértékelést végezni, ezáltal létrejöhet az úgynevezett mintázatok kialakítása.

A mintázatok lényege, hogy ha a terrortámadások bekövetkezésekor megfigyelhető eseménysorok megismétlődnek, akkor ezeket ne felejtse el a rendszer egy következő akciónál, mindvégig maradjon meg a tudás, hogy adott szituációban mik történtek a korábbi eseteknél. Ez segíthet a minél jobb döntések meghozatalában.

Amennyiben az MI megfelelő információk birtokában van, képes meghozni a döntést, amely megállíthatja a ramming-típusú támadást és ezáltal emberéleteket menthet.

A mesterséges intelligencia kutatói a kezdetektől törekedtek különféle programozási nyelvek kialakítására, melyek segítségével leírhatók az MI-k által kezelt információk, illeve feldolgozhatóvá is válnak ezek. A GTMVR rendszer vezérléséhez szükséges egy önállóan dönteni képes szoftver létrehozása, amely akár a meglévő programnyelvek valamelyikén is elkészülhet. Az első mesterséges intelligenciák számára megalkotott nyelv az úgynevezett IPL (Information Processing Language), magyarul információ feldolgozó nyelv volt 1956-ban. Megalkotói Allen Newell, Cliff Shaw és Herbert A. Simon célja az volt, hogy adott információkat képes legyen a gép feldolgozni, tudott dolgozni többek között listákkal, szimbólumokkal, virtuális gépekkel. IPL-t használt több programjuk is, például a híres General Problem Solver (GPS) 1957-ben, amely egy általános célú problémamegoldó szoftver volt, geometriai feladatokat, sakkjátékok lépéseit, teóriák bizonyítását tudta elvégezni és hasonló módon fogott hozzá a részfeladatok megoldásához, mint ahogyan azt az ember is tenné. De ilyen volt még az alkotók saját tervezésű sakkprogramja, az NSS 1958-ban. A Prolog szintén egy nagy múltú programnyelv, amely a relációkat képes egyértelműen leírni az egyszerű logika alapján, ma is széles körben használják.

A történelmi megoldások útját követve eljuthatunk a ma népszerű programnyelvekhez, amelyek szóba jöhetnek, ilyen például a Perl, a Python, amelyeket főleg neurális hálózatok esetében alkalmaznak, de nagyon népszerű a C++ is, mint a C programnyelv továbbfejlesztett változata.

4. Adatbázis

A rendszer adatbázisa gyakorlatilag a fellelhető tudás központja. Könyvtár az MI számára és az irányító hatóság számára is. Míg az MI ebből építkezik, ezek alapján számol és hoz döntéseket, addig az emberi tényező ezekből adatokat tud kinyerni, statisztikákat készíthet, tökéletesítheti a GTMVR egészét.

Az adatbázis kell, hogy tartalmazzon minden tudást, amit a ramming típusú támadásokról a rendszer beüzemeléséig megtudtunk, tartalmaznia kell a GTMVR rendszer pontos leírását, hiszen az MI-nek tudnia kell, hogy mely összetevők hol helyezkednek el, ismernie kell az oszlopokat, a drónokat, a kamerák beérkező adatait, a szenzorok információit. Az adatbázis tehát folyamatosan bővül, ráadásul nem csak a rendszer által fogadott adatokkal, hanem az emberi irányítás is vihet fel újabb és újabb adatokat, amelyekkel gyakorlatilag tovább tanítja és tovább tökéletesíti a GTMVR-t.

Ahhoz, hogy ilyen nagy mennyiségű információ elférjen, célszerű a legkorszerűbb felhőalapú tárolás alkalmazása. A biztonság kérdése persze ugyanolyan fontos, mint a tárolókapacitás vagy az elérés sebessége. Az adatokat titkosítással kell ellátni és az egész adatbázist több körös tűzfal, illetve védelmi mechanizmus mögé rejteni. A sérülések, adatvesztések elkerülése érdekében a legkorszerűbb technológiák alkalmazása szükséges.

5. Kisegítő eszközök

A kisegítő eszközök segítségével fog látni és hallani a GTMVR. Kisegítő eszköznek nevezzük az imént felsorolt öt elemen kívül, a rendszer minden további részét, többek között a kamerákat (normál és éjjellátó üzemmóddal), fotocellákat, lézeres érzékelőket, de ide sorolhatók az útdíjellenőrző, a tengelysúlymérő eszközök, vagy akár a Közúti Intelligens Kamerahálózat (VÉDA), melyeket vagy a már meglévő rendszerekkel történő összekapcsolással, vagy önállóan telepített változataikkal – de képes lenne a rendszer használni. Minél több információ kerül be, annál pontosabb számításokat végezhet az agy, ezért akár az is fontos lehet, hogy az adott jármű milyen tengelyterheléssel érkezik a helyszínre, vagy akár rendelkezik-e érvényes műszakival. A felsorolt külső eszközök tervezésekor fejlesztőik lehetővé tették, hogy más későbbi alkalmazásokhoz kapcsolódhassanak, célszerű lenne a jövőben ezeket bővíteni, frissíteni, hogy egy új rendszerre is felkészülhessenek.

A különböző elemeknek biztonságos vezeték nélküli vagy vezetékes kapcsolaton keresztül kell tudniuk kommunikálni, az ehhez szükséges jeladók és más berendezések szintén a kisegítő eszközök közé tartoznak. Pontosan meg kell határozni, hogy a rendvédelmi szervek milyen specifikációjú berendezéseket fognak tudni használni, illetve hogy melyek azok az elvárások, amelyeknek feltétlenül meg kell felelniük a kisegítő eszközöknek. Számításba kell venni az esetleges bővítés lehetőségét, további sávszélesség kialakítását, más jellegű anyagok továbbítását, gondolok itt például video vagy audiojelre, minden olyan lehetőségre, amely egy bekövetkezett terrorcselekmény kivizsgálásához, a későbbi nyomozáshoz segítséget nyújthat.

Ezen eszközök pontos meghatározása a rendszer kidolgozását megelőző rendszerterv feladata, így ezek felsorolását itt nem teszem meg.

IV. Egy fiktív támadás bemutatása

A legjobb szemléltető eszköz mindig az, ha „élesben” látjuk a rendszer működését. A következő esetleírás tudja talán a legjobban bemutatni hogyan is működik majd a GTMVR. A helyszín a Szent István körút 14. szám alatt található Vígszínház épülete előtti járda. A kiválasztásban szerepe volt annak, hogy egy nem túl felkapott, de időközönként sok ember által látogatott helyszín legyen. Vannak forgalmasabb és ezáltal veszélyeztetettebb területek, például hidak, terek vagy sétálóutcák, ám a GTMVR felépítése lehetővé teszi, hogy egy kisebb forgalmú, de ugyanúgy veszélyeztetett közterületet is megvédjen. Emiatt került a választás erre a területre.

Délután fél 5-kor rengeteg ember várakozik a Vígszínház előtti kis téren, mindannyian az 5 órai előadásra várnak. A Jászai Mari tér felől még több néző igyekszik a színház elé, a Nyugati tér felől pedig járókelők haladnak. A GTMVR rendszer kamerái érzékelik a színház előtt megnövekedett emberi jelenlétet, az információ rögzítésre kerül. Pár perc múlva a Hegedűs Gyula utca magasságában egy személygépkocsi közlekedik a jobb oldali buszsávban, amely tilosban haladás már önmagában felkelti a rendszer érdeklődését, pár pillanattal később a rendszer regisztrálja, hogy az autó felgyorsít. Az MI tudja, hogy a kanyarodásra felkészülve a járműnek használnia kellene az irányjelzőjét, illetve lassítania kellene, így a rendszer veszélyesnek minősíti a védett zóna felé haladó autót. Alig telik el pár ezredmásodperc, amikor az autó vezetője jobbra rántja a kormányt, ezáltal az autó orra a védett zóna felé irányul. A veszélyes besorolású gépjárművet a felismerést követően szinte azonnal támadó járművé minősíti a gépi intelligencia, majd megkezdi a gépjármű előtt elhelyezett oszlopok felemelését, valamint a sebesség és a hátralévő távolság miatt egy hátrébb elhelyezett oszlopsor felemeléséről is dönt. Ugyanebben a pillanatban a közeli villanyoszlopra erősített drónrekeszből kirepül két elhárító drón és a közeledő autó felé repül. Az autó vezetője érzékeli az emelkedő akadályokat, kitérni azonban képtelen, így a gépjárművel egyenesen az emelkedő védelmi eszközöknek rohan. Az autó eleje kis mértékben meggyűrődik és fennakad két oszlopon. Abban a pillanatban, amikor a támadó sofőr kinyitja a sérült gépjármű ajtaját, az egyik drón az autó oldalával egy vonalba kerül és információit továbbítja az MI számára. A villámgyors kiértékelést követően – mely szerint a gyanúsított lőfegyvert tart a kezében – a drón megfelelő mértékű lézerlövéssel semlegesíti a támadót. A férfi összecsuklik a volán mögül kiesve és a földön rángatózik. Már nem tudja használni lőfegyverét, melyet a drón a biztonság kedvéért szintén semlegesít egy jól irányzott tűlövedékkel. Ez alatt az idő alatt a kettes drón az autó túloldalán tartózkodott, felmérte, hogy nincs másik utas a gépjárműben. 1 perc 22 másodperc múlva a helyszínre érkezik a legközelebbi járőr egység, akiket a rendszer a támadás felismerésének pillanatában riasztott. A rendőrök őrizetbe veszik a férfit, eközben a GTMVR figyelmeztető hangjelzés mellett felengedi a többi oszlopot, elkerülendő egy következő támadást. Előfordulhat ugyanis, hogy egy adott helyre több terrorista érkezik más-más járművel.

A helyszínelés ideje alatt megérkezik egy GTMVR szakértő/kárfelmérő kolléga, aki helyi szinten is ellenőrzi a berendezésben bekövetkezett változásokat, sérüléseket, valamint diagnosztizálja az egységek állapotát.

1. Az eset kiértékelése

A fiktív eseménysor megírása közben számomra is nehéz volt minden apró részletet megjegyezni, ami ezredmásodpercek alatt zajlott a védelmi rendszer elemei között. Az MI tervezésekor sokkal bonyolultabb és összetettebb leírás szükséges a lehetséges funkciók és állapotok pontos bemutatására. Több egymással összefüggő, egy időben történő eseményre nem tértem ki az ismertetés során, csupán szemléltetni igyekeztem egy lehetséges akció kimenetelét.

Jól látható volt, hogy a közeledő veszély felkeltette a gépi intelligencia érdeklődését, majd a bekövetkezett támadás során a döntést azonnal képes volt meghozni és az elhárításnak megfelelő mértékű intézkedést foganatosítani. A hatékonyságot persze több tényező befolyásolja, ám a rendszer kialakításakor minden egyes megvalósítási helyszínen az adott területre jellemző lehetőségeket figyelembe véve kell telepíteni az eszközöket. A megjelenített helyszínen például a buszsáv a rendszer segítségére volt, hiszen ott alapesetben nem közlekedhetnek civil járművek, ráadásul, ha bekanyarodnak, akkor ahhoz is megfelelő jelzést kell, hogy használjanak. Ezeket a támadó elmulasztotta, majd láthatóan támadó szándékkal gyorsított és bekanyarodott.

Felmerülhet a kérdés, hogy mi történik, ha mindez egy olyan járművel esik meg, amely nem támadó szándékkal vált irányt, hanem például meghibásodás, vagy a sofőr rosszulléte miatt? Ebben az esetben a rendszer ugyanígy viselkedett volna és megakadályozta volna az emberek közé csapódó irányíthatatlanná vált járművet. A különbség akkor fedezhető fel, amikor a kirepülő drónok felmérik a lehetséges támadó sofőrt, majd kiértékelve a helyzetet – például azt, hogy az illető nem támad, nem rendelkezik fegyverrel, illetve esetleg rosszul van – a rendőrök után mentőket is a helyszínre kérnek. Így a hátrány előnnyé válhat, és bár sajnálatos, hogy az oszlopoknak csapódott a rosszul lévő sofőr, ám a drónok segítségkérése által hamarabb kerül majd kórházi kezelés alá.

Ezen a ponton nagyon érdekes kérdés a támadó szándék felismerése, vajon minden esetben, amikor a rendszer reagál, egy terroristát akadályoz meg? Elképzelhető olyan eset, amikor vétlen sofőrök „esnek áldozatául" a rendszernek? Véleményem szerint ennek kicsi a valószínűsége, elvégre bármilyen esemény okozza is a tömegbe hajtást, legyen szó valódi terrortámadásról vagy szimplán csak egy meghibásodásról, rosszullétről, a végeredmény ugyanúgy a járókelők biztonságát szolgálja. Kimondhatjuk tehát, hogy a GTMVR rendszer a terrorcselekmények megakadályozásán túl közlekedésbiztonsági eszközként is kiválóan használható.

V. Lehetséges problémák

Egy ilyen komplex rendszer üzemeltetése során számos problémába ütközhetünk, a teljesség igénye nélkül, az egyes elemeken végighaladva megpróbálom összesíteni melyek a legfontosabbak.

Az oszlopok tekintetében van talán a legkönnyebb dolgunk, ezek az eszközök jóval egyszerűbben működnek, mint a rendszer további elemei. A kiemelkedésnél és

földbe csúszásnál azonban többről van szó. Mi történik akkor, ha egy járókelő túl közel van egy oszlophoz, vagy egy oszlop fölött áll, esetleg egy oszlop és a támadó jármű közé kerül? A kérdés ebben az esetben, hogy milyen módszert adjunk az MI kezébe a helyzet megoldására? Mit kell először figyelembe vennie? Esetleg azt, hogy az oszlop fölött tartózkodó személy valószínűleg megsérül, ha az elem hirtelen kiemelkedik? Ha ebben az esetben inkább nem emeli fel az oszlopot, de közeledik a jármű, lehetséges, hogy nem fogja tudni megállítani a járművet és további emberek esnek áldozatul. Ugyanakkor az is előfordulhat, hogy az illető éppen elugrana a közeledő jármű elől, amiben aztán a felemelkedő oszlop akadályozza meg. Úgy gondolom, hogy a helyes megoldás minden esetben az lehet, amivel az esetleges támadáskor több ember életét tudjuk megmenteni. A morális kérdésen túl egy ilyen eset jogilag is kérdőjeles, a rendszer megalkotásakor viszont muszáj ezt is figyelembe venni.

A drónok szabályozása aktuális téma mind a Nemzeti Fejlesztési Minisztérium Közlekedési Hatóságainál, mind pedig a Terrorelhárítási Központnál. A TEK álláspontját figyelembe véve, mely szerint: *„Az eszközöket kategóriától függően elektronikus vagy vizuális gyári számmal kell ellátni az azonosítás érdekében. Méretre, tudásra való tekintet nélkül engedélyhez és/vagy regisztrációhoz kell kötni, az eszközt, a felhasználót, és minden egyes repülést is."*[6] – fontos, hogy a beépítésre kerülő gépek azonosíthatóak legyenek, az adatbázisban rögzítésre kerüljön minden egyes repülésük, beleértve a tesztüzemeket is. Felmerülő kérdés, hogy vajon ezek az UAV-k mennyi önálló intelligenciával kell, hogy rendelkezzenek? Maguk a drónok fogják például felismerni a rendvédelmi szerv munkatársát, vagy mindezt az MI-re bízzuk és így a drón csak a központi agy egy hardvere lesz, minimális önállósággal? Még érdekesebb kérdés, hogy vajon mi alapján kerülnek azonosításra a rendvédelmi dolgozók? Egy helyszínre érkező rendőrről mi alapján állapítja meg az MI, hogy ő valóban az, akinek mondja magát és nem egy álrendőr? A terrorista társa például, aki rendőrnek adja ki magát. Az azonosíthatóság szintén kényes kérdés, hiszen egyrészt a munkatárs védelme is fontos, másrészt biztosítani kell számukra a munkajog által megszabott jogokat. Nem lehet csak úgy felcímkézni vagy chippel ellátni a rendvédelmi szerv személyzetét, igaz? Viszont a gépnek tudnia kell, hogy ki ellenség és ki barát. A legjobb megoldás valószínűleg a biometrikus azonosítás, például az arcfelismerés. Földesi Krisztina Doktori értekezése hivatkozik a két alapvető módszerre, egyik a *„minta alapú (vagy fotometrikus). Ennek lényege, hogy az arc, vagy arcrészletek (szem, ajkak, orr) globális tulajdonságait vetik össze a letárolt mintával, mintákkal."* a másik pedig a *„geometriai (az arc különböző részleteinek szem, ajkak, orr, áll, stb. – egymáshoz viszonyított elhelyezkedését és méretét elemzik)."*[7] Az arcfelismerésre képes drón meg tudná határozni a kiérkező kolléga személyazonosságát, és ezáltal meggyőződne róla, hogy az nem az elkövető társa.

A gépi agy, avagy az MI okozhatja a legnagyobb fejfájást, amennyiben problémákról beszélünk. Akárcsak az önvezető autók esetében, felmerül a kérdés, hogy milyen helyzetben hogyan döntsön a gép? Azt gondolom, hogy a helyzet nem

---

[6] BECK Attila: Az UAV-k polgári alkalmazásának kockázatai, és kezelésük lehetséges módszerei terrorelhárítási és személyvédelmi szempontból. Terror & Elhárítás. 4. évfolyam 2015/2., p. 78.

[7] FÖLDESI Krisztina: A biometrikus azonosítási eljárások alkalmazhatósága a rendőri munkában. Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest, 2017.

ennyire bonyolult amikor ramming típusú terrorcselekményekről beszélünk. A mérlegelés mértéke jóval kevesebb és így a kockázat is alacsonyabb. Itt nem arról van szó, hogy helyesen dönt-e az MI, amikor megakadályozza a támadást, vagy semlegesíti az elkövetőt. Maga az esemény felismerése jelenthet hibaforrást, ez pedig nem az MI maga, hanem inkább a mögötte álló adatbázis, vagy a beérkező adatok helyessége. Ha létre tudjuk hozni azt, ami a célunk, egy olyan önállóan gondolkodni képes programot, amely a beérkező információk alapján megakadályozza a ramming-típusú terrortámadást, sok gondunk nem lesz vele. Miben azonosíthatók mégis a problémák? Hibás vagy hiányos adatokban, fals információk miatt hozott rossz döntésekben. Ha feltételezzük, hogy magának az MI-nek a programozása, a mechanizmusa hibátlan, akkor – akárcsak az ember esetében – a beérkező információkban lehet probléma.

Egy, az elvárásoknak megfelelő szoftver létrehozása hatalmas kihívás, számtalan specifikációnak meg kell felelni a biztonságon át a döntésekhez szükséges rutinokig. Jelen korban, úgy gondolom, nincs lehetetlen ezen a téren. A műszaki tudományok és a technológia elvitathatatlan fejlődésen ment keresztül az elmúlt évtizedekben, nyilvánvalóan sok nehézséget kell leküzdeni, de a feladat nem lehetetlen.

Az adatbázis hibalehetőségeiről az imént már ejtettem néhány szót, a lehető legkisebb hibaszázalékkal szabad dolgozni, a hibás adatokat időről időre szűrni kell, hogy az MI minél jobb munkát végezhessen. A kamerák és szenzorok gyermekbetegségeit enyhíteni kell, úgy mint az éjszakai üzemmódok, a hőképek vagy éppen a különböző megtévesztések, amelyek alapján hibás adatok kerünek rögzítésre, vagy hiányossá válik az információ.

Az adatvesztés elkerülése érdekében érdemes duplikált adatokkal dolgozni, a megfelelő biztonsági másolatok megléte elengedhetetlenül szükséges. Fel kell készülni az esetleges vészhelyzetekre, akárhol legyen is a szerver, vagy akárhol legyenek az adatok a felhőben tárolva, fontos, hogy az összegyűjtött állományok sebezhetősége minimálisra csökkenjen.

Az adatvesztés vagy a hibás adatok gyakran a kamerák, szenzorok hibájából erednek, esetleg a hálózaton elveszett adatcsomagok miatt, így különös figyelmet kell fordítani a biztonságra, a rendszer alkotóelemeinek karbantartására, rendszeres ellenőrzésére. Nagyon fontos, hogy a bekövetkezett terrorcselekményt követően a lehető leghamarabb ismét működőképessé váljon a rendszer az érintett területen.

Habár költségtervet nem terveztem készíteni eme tanulmányomhoz, az ilyen jellegű, sok mindenre kiterjedő fejlesztés nem olcsó dolog. A GTMVR azonban nem rövidtávú lehetőség, hanem inkább egy jövőbeli cél, egy lehetséges útja a rendvédelemnek, amelyet célszerű több más hasonló kezdeményezéssel összevontan kezelni. Egy okosvárosról szóló terv egyik témájaként bőven van potenciál a rendszerben, egy nagyobb beruházás keretében valószínűleg könnyebb lehetne a finanszírozása is. Érdemes végiggondolni, hogy mely városok mely konkrét pontjai vannak leginkább kitéve az ilyen jellegű cselekményeknek, mely épületek vagy közterületek azok, amelyeket célszerű lenne ilyen megoldással védeni. A tudatos építkezés, melynek során például a buszmegállók, terek már a tervezés szintjén

elkülönülnének a közúttól, jelenthet-e megoldást a problémára, vagy marad-e olyan terület, ahová mégis inkább a GTMVR lenne kézenfekvőbb megoldás.

VI. Összegzés

A GTMVR egy olyan komplex rendszer, amely nagy biztonsággal tudja felvenni a harcot a ramming-típusú terrortámadásokkal szemben, teljes körű védelmet nyújt a támadó gépjárművek ellen azáltal, hogy mind a mechanikus, mind pedig a beavatkozó drón vezérlését is képes megoldani, illetve párhuzamosan képes értesíteni a hatóságokat, legjobb esetben a legközelebbi bevethető rendvédelmi munkatársat. Értékelő és elemző rendszere, illetve mindenre kiterjedő adatbázisa révén rendelkezik minden olyan információval, amely a megfelelő önálló döntéshozatalhoz szükséges, továbbá tanulásra képes, önfejlesztő, hatékonysága így exponenciálisan növekszik.

Öt eleme a földbe süllyesztett oszlopok, amelyek kiemelkedése megakadályozza a támadó autóval történő behajtást, a drónok, amik a gyanúsított további cselekedeteit akadályozzák meg. Az MI vezérli a teljes rendszert, a beérkező információkat kiértékeli és ezek alapján döntéseket hoz. Az adatbázis tartalmazza az összes információt, rendszerezve, megfelelő logikai elvek alapján tárolja a rendszer tudását, míg a kisegítő elemek jelentik a rendszerbe beérkező adatok forrását, úgymint a kamerák, szenzorok, érzékelők, sebességmérők, esetleg más külső rendszerek adatai, például a VÉDA rendszerből, vagy a tengelysúlymérő kapuk által.

A GTMVR üzemeltetéséhez szükséges egy felügyelő szervezet, ami a jogi szabályozás alapján a hatósági feladat ellátására jogosult, szükséges informatikai és egyéb technológiai támogatás, kell hogy legyen olyan szakértő, aki ismeri a rendszer működését, felépítését, ért a javításához. A megfelelő back-office segítségnyújtás nélkül egy ilyen rendszer nem képes üzemelni. Mivel egy teljesen új szisztémáról van szó, különös figyelmet kell fordítani az oktatásra, a rendszert meg kell ismertetni a rendvédelmi használók körével, hogy a jövőben hatékonyan együtt tudjanak dolgozni, ismerjék a rendszer feladatát, annak lehetséges reakcióit, kockázatait. Kiemelten fontos, hogy a rendvédelmi dolgozók, akik közvetlenül is kapcsolatba kerülhetnek a GTMVR-ral tisztában legyenek a működési elvével. Nem kell azonban rideg gépnek tűnnie, hiszen egy bizonyos fokig önmagában is dolgozni képes MI-ről van szó, ami nem csupán egy felhasználót segítő digitális eszköz, hanem egy kialakított védelmi rendszer szerves eleme. Marketing szempontból is megkönnyítené egy ilyen rendszer bevezetését, ha kapna valamilyen becenevet. Ezáltal személyesebbé válhat a kapcsolat az ember és gép között, az emberi intelligencia és az azt segítő gépi intelligencia között. A munkatársak számára nem egy elérhetetlen szoftver lenne, hanem egy konkrét munkatárs lenne ez a komplex védelem.

Bár jelen írásomban nem beszélünk valódi MI-ről – elvégre a technológiai fejlődés ezen szakaszában valódi, ember módjára gondolkodni képes MI-t még nem tudunk megalkotni – azonban érdekes lenne belegondolni, hogy egy valódi MI-ként létező védelmi rendszer gyakorlatilag nem egy gép lenne, hanem konkrétan az ember egyik munkatársa. Neki is meglennének a jól elhatárolt feladatai, feladatköre,

mely szerint cselekedve végezné munkáját. A Zsigmond Király Főiskolán írt szakdolgozatom[8] végén felmerült az a kérdés, hogy vajon egy valódi MI minek számít? Vajon egy az emberrel teljesen megegyezően gondolkodó gép gépnek számít-e a továbbiakban? Vajon egy ilyen dolog már emberré válik-e, ha teljesen ugyanúgy tud gondolkodni, mint mi? Például, ha mi legyártunk egy ilyen MI-t, akkor az a mi tulajdonunk maradhatna-e, még akkor is, ha az szabadon gondolkodni képes? Ő mit akarna?

Ez a gondolat annyiban kapcsolódik a jelenlegi dolgozathoz, hogy egy védelmi rendszernek nem szabad, hogy a saját világán kívül, a saját megszabott keretein kívül önálló akarata legyen. Nem beszélünk tehát – ma még megvalósíthatatlan – valódi MI-ről, csupán egy jól meghatározott világon belül létező intelligenciáról, amely a saját feladatkörében – gázolás megakadályozása a megadott eszközökkel – tevékenykedik. Úgy érzem, addig vagyunk biztonságban, amíg az MI csak a saját hatáskörén belül tud dönteni vagy gondolkodni. Amint egy gép ugyanúgy képes lenne átgondolni helyzetét, ahogyan azt mi emberek tesszük, felvetődik a kérdés, hogy miért akarna például nekünk segíteni? Ha saját maga gondolkodik, miért pont mi lennénk azok, akikhez lojális maradna?

VII. Jövőkép

Bármerre is nézünk a világban, a fejlődés az élet minden területén tetten érhető. Egyre-másra születnek olyan ötletek, melyek városainkat is modernizálják. 10 évvel ezelőtt még nem volt a metróalagútban internetes kapcsolat, ma viszont már hibátlanul üzemel. Terjednek az okosvárosokról szóló publikációk, de ugyanígy hatalmas fejlődésen megy keresztül az önvezető járművek építése. Henry Ford és Galamb József T-modelljének piacra kerülésével 1908-ban köszöntött be az olcsó és megbízható autók korszaka. *„Joe, van egy ötletem. Tervezzünk egy új kocsit. Vigye a rajztábláját egy külön szobába, hozzákezdünk egy új modell tervezéséhez. Nem kell róla tudni senkinek. Az első dolog, hogy új sebességváltó kell, mert az eddigiekkel elégedetlen vagyok, nem elég praktikus…" szólt Ford az ijfú Galamb Józsefhez.*[9] Mára pedig már ott tartunk, hogy Ágó Béla, a Ford CEE Warranty and Quality Manager-e a Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karon 2017. október 27-én zajlott Ford emlékülésen elhangzott előadásában a Ford vezető szerepét emelte ki az önvezető autók gyártásának területén.[10] Hamarosan olyan gépjárművek jöhetnek, amelyek képesek lesznek a városokban közlekedni, figyelembe venni a közlekedési szabályokat, figyelni tudják a környezetüket, reagálnak majd a körülöttük haladó járművekre, kerékpárosokra, gyalogosokra. Eléggé úgy tűnik, hogy ez jelenti a jövőt. Éppen ezért, egy ilyen környezetben, ahol már maguk az utak és a rajtuk közlekedő autók is ezt az irányt képviselik, a védelmi rendszerek sem tűnnének ki környezetükből. Esztétikailag nem rombolják a város látképét, gondos tervezésüknek köszönhetően a berendezéseik illeszkednek az utca

---

[8] HASILLÓ György: A mesterséges intelligencia. Zsigmond Király Főiskola Kommunikáció- és Művelődéstudományi Intézet. 2011.

[9] Dr. GÁTI József: „Kerekekre teszem Amerikát!" - Henry Fordra emlékezve (előadás). Ford Emlékülés az Óbudai Egyetemen. Óudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 2017. 10. 27.

[10] ÁGÓ Béla: Milyen lehet a XXI. század autója? Ford Emlékülés az Óbudai Egyetemen. Óudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 2017. 10. 27.

stílusához, ugyanakkor belső alkatrészeik a hatékonyság jegyében kerülnek összeállításra, sőt, a trendeknek megfelelően elsősorban alternatív forrásokból biztosítanák a működésükhöz szükséges energiát. A rendszer akkor lesz igazán innovatív, ha minden eleme, alkatrésze, minden vele kapcsolatos berendezés az új technológiai vívmányoknak megfelelően készül, ha minden alkotóeleme jövőbe mutató.

VIII. Záró gondolatok

A GTMVR egyedülálló rendszer lehetne, mely elképzelés megvalósítása előtt érdemes feltérképezni a nemzetközi helyzetet, fontos az összhang megteremtése az európai álláspont és a hazai nemzetbiztonsági és biztonságpolitikai ötletekkel, a nemzeti kiberbiztonság céljaival és feladataival. Érdemes lenne megvizsgálni ezen területek hazai helyzetét, mind a politikában, mind az oktatásban, hogy az újonnan kialakításra kerülő megoldásokkal az abban résztvevő szereplők és a jövőbeli felhasználók is tájékozottak lehessenek.

Írásom célja, hogy még ha csak elméleti szinten is, de új ötletek és kérdések felvetésével, új megoldások keresésével, innovatív, jövőbe mutató eszközök bevonásával segítséget nyújtsak a rendvédelmi szervek jövőbeli tevékenységéhez, a gépjárművekkel elkövetett borzalmas merényletek megakadályozásában, melyek ártatlan emberéleteket veszélyeztetnek szerte a világon.

Felhasznált irodalom:

- ÁGÓ Béla: Milyen lehet a XXI. század autója? Ford Emlékülés az Óbudai Egyetemen. Óudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 2017. 10. 27.
- BECK Attila: Az UAV-k polgári alkalmazásának kockázatai, és kezelésük lehetséges módszerei terrorelhárítási és személyvédelmi szempontból. Terror & Elhárítás. 4. évfolyam 2. szám 2015/2., p. 78.
- FÖLDESI Krisztina: A biometrikus azonosítási eljárások alkalmazhatósága a rendőri munkában. Óbudai Egyetem Biztonságtudományi Doktori Iskola. Budapest. 2017.
- Dr. GÁTI József: „Kerekekre teszem Amerikát!" - Henry Fordra emlékezve (előadás). Ford Emlékülés az Óbudai Egyetemen. Óudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 2017.10.27.
- HASILLÓ György: A mesterséges intelligencia. Zsigmond Király Főiskola Kommunikáció- és Művelődéstudományi Intézet. 2011.
- Merriam Webster Dicitionary: Intelligence. https://www.merriam-webster.com/dictionary/intelligence (Letöltés ideje: 2018. 01. 02.)

- RÁCZ András – BRESTYÁNSZKI Flóra: A gépjárművel végrehajtott, ramming típusú terrortámadásokról és a védekezés lehetőségeiről. http://archiv.netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-14-a-gepjarmuvel-vegrehajtott-ramming-tamadasokrol-racz-a-brestyanszki-f.original.pdf (Letöltés ideje: 2017. 12. 01.)
- Transportation Security Administration Office of Security Policy and Industry Engagement Surface Divison - Highway and Motor Carrier Section: Vehicle Ramming Attacks Threat Landscape, Indicators, and Countermeasures May 2017. https://publicintelligence.net/tsa-vehicle-ramming/ (Letöltés ideje: 2017. 12. 05.)

PUSKÁS ADRIENN

A NATO ÉS EU KIBERVÉDELMI POLITIKÁJÁNAK ÁTTEKINTÉSE

„Az Internet az első dolog, amit az ember épített, s amit mégsem ért. Ez a valaha volt legnagyobb kísérlet az anarchiára."[1]
Eric Emerson Schmidt

Bevezetés

1947 és 1991 között a hidegháború hatására nagyfokú haditechnikai fejlesztés indult az Egyesült Államokban. Ennek keretein belül 1958-ban az Amerikai Védelmi Minisztérium létrehozta az ARPA[2]-t. Paul Baran 1964-ben egy olyan hibatűrő rendszer létrehozását tűzte ki célul, amely védett a külső támadások ellen. Így a centralizált hálózat helyett az elosztott hálózatot szorgalmazta. Bár az ötletét először elvetették, 1969-ben létrehoztak egy kísérleti hálózatot, amelynek tesztelésében egyetemek vettek részt. A szolgáltatás nagy népszerűségre tett szert és elindult az internet robbanásszerű fejlődése. Azonban nem Baran elképzelése, hanem egy skálafüggetlen modell kezdett kialakulni. Az internet népszerűsége egyre nőtt, az intézmények sorra csatlakoztak hozzá. Létrejött egy véletlen hibákkal szemben is ellenálló komplex rendszer, azaz a ma ismert internet.

Mára mindennapjaink meghatározójává vált az internet. Létrejöttével munkamódszereink és életvitelünk gyökeres változáson ment keresztül. A technikai fejlődés hatására vásárlásainkat otthonról, pár kattintással kivitelezhetjük, csekkjeinket a digitális platformon keresztül fizethetjük be, a több ezer kilométerre történt politikai, katonai eseményekről pár perc alatt informálódhatunk. Ezek mellett a technikai fejlődés és digitalizálódás az oktatásra, egészségügyre, közigazgatásra, gazdaságra és katonai rendszerekre is nagy hatást gyakorolt, amelyek működése elképzelhetetlen mára az internet nélkül.

Mi történik azonban akkor, ha az általunk használt digitális platformot egy olyan támadás éri, amely akár egy egész állam megbénítását képes okozni? Hogyan reagál az Európai Unió és a NATO egy olyan katasztrófahelyzetben, amikor a kritikus infrastruktúrák megbénulnak? Fel vannak készülve az EU tagországok egy kibertérben történő támadás ellen?

Napjainkban az Európai Unió globális biztonságát egyre több tényező fenyegeti. Gondolhatunk itt az egyre égetőbb problémaként megjelenő migrációra, az energiabiztonság megteremtéséért való küzdelemre, az európai társadalom elöregedésével bekövetkező demográfiai változásra. Ezek mellett azonban új kihívásként jelenik meg a kibertér egyre növekvő szerepe miatt a elektronikus információs rendszerek biztonsága.

[1] https://www.citatum.hu/szerzo/Eric_Emerson_Schmidt (Letöltés ideje: 2018. 02. 05.)
[2] Advanced Research Project Agency

Fogalmi áttekintés

A témám pontos értelmezése miatt fontosnak tartom az általam használt alapdefiníciókat meghatározni.

A NATO és az Európai Unió egyik legfontosabb céljai közé tartozik a tagországai biztonságának megteremtése. De mit jelent manapság a biztonság és mik veszélyeztetik azt?
„A biztonság a társadalom belső viszonyaiban kifejezi azt az állapotot, amikor az egyes társadalmi alrendszerek funkciók szerint, szabályozottan működnek és működésüket semmilyen immanens veszély nem zavarja."[3]

Az IT-forradalom, a technikai fejlődés és az internet egyre nagyobb népszerűsége miatt az információs biztonságra is nagyobb figyelmet kell fordítani.
Az információs biztonság alatt a következőt értjük: *„az információk védelme a véletlen, vagy szándékos jogosulatlan megismerés, továbbítás, módosítás vagy megsemmisítés ellen. Megj.: Az információ létezhet az emberi agyban, dokumentum formában és elektronikus formában…"*[4]

A kibertér mára egy minden területen (pl.: katonaság, gazdaság, politika) megjelenő fogalommá vált, alkalmazásának kiterjedése miatt így egységes definíció nem létezik.
Kovács László az erről szóló tanulmányában a következőképpen determinálja a fogalmat: *„Felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva."*[5]

A NATO pedig a következő definíciót használja: *„a kibertér egy komplex dinamikus környezet, a működési környezet (operating environment) egyik összetevője"*[6]

Katonai szempontból elengedhetetlen az USA hadereje által használt fogalom ismerete, ami a következőképp hangzik: *„…a kibertér az információs környezet (information environment) részét képező globális tartomány (domain), ahol az információs környezet az információt gyűjtő, feldolgozó, terjesztő, és felhasználó személyek, szervezetek, és rendszerek összessége, a tartomány kifejezés pedig hadviselési tartományt (warfighting domain) jelöl."*[7]

A virtuális tér egyre növekvő szerepe miatt jött létre a kiberbiztonság fogalma, ami a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján a következő: *„A kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai,*

---

[3] ÜRMÖSI Károly: A biztonság, a biztonság fogalma; Hadtudományi Szemle, 2013/4. p. 148.
[4] MUNK Sándor: Információbiztonság vs informatikai biztonság; Hadmérnök, 2007/különszám p. 12.
[5] KOVÁCS László: A kibertér védelme; Budapest, Dialóg Campus Kiadó 2018a. p. 18.
[6] MUNK Sándor: A kibertér fogalmának egyes, az egységes értelmezését biztosító kérdései; Haditechnika, 2018/1. p. 115.
[7] Uo.

jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."[8]

Mára a globalizáció, a digitalizáció és az információ felgyorsulásának következtében megváltoztak az érdekek és az érdekérvényesítések is. A gazdaság és a politika mellett a katonaság is változáson ment keresztül ennek köszönhetően. Új hadviselési formaként jelent meg a hibrid hadviselés, illetve az aszimmetrikus hadviselés.[9]
„A hibrid hadviselés a hagyományos reguláris (lineáris, konvencionális) és az irreguláris (nem lineáris, nem konvencionális) hadviselés puha, közepes és kemény módszereinek, eljárásainak rugalmas alkalmazása abból a célból, hogy az ellenség államát, fegyveres erőit működésképtelenné, védtelenné tegyük és akaratunkat rákényszeríthessük, legfőképpen azzal a stratégiai céllal, hogy az erőszak szintje a konfliktus folyamán ne haladja meg a háborús szintet".[10]

Aszimmetrikus hadviselés alatt pedig a következőt értjük: *„Pontosan körvonalazott politikai célok érdekében folytatott, gyakran több szervezet ideológiai, vallási, etnikai közösségén alapuló katonai, és nem katonai műveleteket, eljárásokat és módszereket alkalmazó közvetlen és közvetett hatásokra építő és egymás hatásait felerősítő, a biztonság különböző dimenziónak területét veszélyeztető harcmodor, főként harcászati eljárás, melyek együttes hatásával kényszeríthetjük akaratunkat az ellenségre."*[11]

A fentieket hangsúlyozza Magyar Sándor és Simon László is: *„A terrorizmus elleni erőfeszítések esetében a hagyományos fegyveres műveletek mellett a kibertér is egyre hangsúlyosabban jelenik meg mind a támogató, mind az önálló műveletek végrehajtásának színtereként. Ez a tendencia tudatos felkészülést követel meg a védelmi képességek kialakítása területén is. A hibrid hadviselés, az információs műveletek korában az egykor kiszolgáló támogató területek, mint a híradás és az informatikai üzemeltetés szerepe felértékelődik."*[12]

A fejlett országok, melyek a fejlődés következtében megjelenő új eszközöket jól alkalmazzák, óriási privilégiummal rendelkeznek. Az információk gyors megszerzésével, majd azok hatékony felhasználásával olyan információs előnyre tesznek szert, amely nagy mértékben befolyásolja az államok közötti diplomáciai kapcsolatokat háborúban, illetve békeidőben egyaránt. Éppen ezért vált szükségessé

---

8 A hálózati és információs rendszerek biztonságára vonatkozó Stratégia, http://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf, p. 3. (Letöltés ideje: 2018. 02. 05.)

9 PUSKÁS Béla: A diplomácia és a virtuális tér kapcsolata; Felderítő Szemle 2018/3. pp. 39-55.

10 RESPERGER István: A válságkezelés és a hibrid hadviselés; Budapest, Dialog Campus 2018. p. 21.

11 RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban; Budapest, Zrínyi Kiadó 2014. p. 23.

12 MAGYAR Sándor – SIMON László: A terrorizmus és indirekt hadviselése az EU kiberterében, Szakmai Szemle: 2017/4. p. 65.

a kritikus infrastruktúrák, különös tekintettel a kritikus információs infrastruktúrák[13] védelme. Ezek alapján fontos e két, napjainkban gyakran használt kifejezést tisztázni.

Az Országos Katasztrófavédelmi Főigazgatóság a következőképpen határozza meg a kritikus infrastruktúrát: *„…egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtő, a gazdaság működését elősegítő vagy lehetővé tévő azon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége vagy ezek részei, amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkent szintje egy adott felhasználói kör létére, lét- és működési feltételeire negatívan hat."*[14]

Szinte minden kritikus infrastruktúra vezérléséhez, ellenőrzéséhez és irányításához valamilyen infokommunikációs eszköz szükséges. Így tehát egy adott állam technológiai alapú infrastruktúrájának működése nagyban befolyásolja az állam működését. Ennek következtében az információs infrastruktúrák a kritikus infrastruktúrák részét képezi.[15]

A 2005-ös európai program Zöld könyve a következőképpen határozta meg a kritikus információs infrastruktúrát: *„Kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak stb.)."*[16]

Kibervédelmi stratégia a NATO-ban

A 2007-es tallinni események hívták fel a NATO és az EU figyelmét az információs hadviselés egyre növekvő szerepére. Észtország ebben az évben egy több mint két hétig tartó kibertámadás áldozatává vált. Az akciók során a támadók megbénítottak több kritikus infrastruktúrát, többek között a kormány honlapját is, ahol hamis információkat jelenítettek meg. Emellett órákon át elérhetetlenné vált az internetszolgáltatás az egész ország területén, a parlament, a hivatalok, a bankok szerverei leálltak. A Hansa bankot a támadás következtében több mint egy millió dolláros kár érte. Ez az úgynevezett DDoS[17] internetes támadás volt a NATO megalakulása óta az első, nem fizikai térben zajló konfliktus. A NATO-t felkészületlenül érte a támadás, a válaszlépés számos kérdést vetett fel. 1949-es Észak-Atlanti Szerződés kimondja, hogy amennyiben az egyik tagországot támadás éri a NATO köteles reagálni.

---

13 Kritikus infrastruktúra: A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben ez a fogalom, mint létfontosságú rendszerek és létesítményekként szerepel.

14 http://www.katasztrofavedelem.hu/index2.php?pageid=lrl;

15 VARGA Péter János: A kritikus információs infrastruktúrák értelmezése; Hadmérnök, 2008/3. pp. 149-156.

16 Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final; https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52005DC0576&from=EN (Letöltés ideje: 2018. 02. 05.)

17 Distributed Denial of Service – a DoS támadások egyik válfaja, az ún. elosztott támadás

Az 5. cikkelyben foglaltak szerint: *„A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek és ennél fogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben azonnal megteszi azokat a intézkedéseket – ideértve a fegyveres erő alkalmazását is –, amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart. Minden ilyen fegyveres támadást és ennek következtében foganatosított minden intézkedést azonnal a Biztonsági Tanács tudomására kell hozni. Ezek az intézkedések véget érnek, ha a Biztonsági Tanács meghozta a nemzetközi béke és biztonság helyreállítására és fenntartására szükséges rendszabályokat.”*[18]

Viszont egy kibertérben történő támadásra nem volt sem a NATO, sem az EU felkészülve, így válaszlépésre még sem került sor. A tallinni események után nyilvánvalóvá vált, hogy egy kibertámadás békeidőben is képes óriási károkat okozni, és akár egy hagyományos támadás előfutárának is lehet tekinteni. Ezt felismerve a NATO megtette az első lépést a tagországai kiber-kapacitásának növelése érdekében és létrehozta a szövetség Kibervédelmi Kiválósági Központját[19] Tallinnban. 2010-ben a lisszaboni NATO-csúcstalálkozó alkalmával új stratégiát fogadtak el, amelyben megtalálható a katonai híradó- és informatikai rendszerek védelme is. Az új stratégia három fő jeligén alapszik: kooperatív biztonságon, válságkezelésen és kollektív védelmen. 2011-ben pedig egy új kibervédelmi stratégiát is alkottak, amelyben már egy cselekvési terv is szerepel. 2012-ben további fejlesztések születtek a kibertámadásokkal szembeni ellenállás fejlesztése érdekében. Ebben az évben indult el ugyanis a NATO kiberincidens-kezelési képességének[20] és a kiberfenyegetés-előrejelző központnak[21] a kiépítése.

A 2014-es walesi NATO-csúcs során a NATO-tagállamok logisztikai, vezetés-irányítási, kibervédelmi és az ukrán haderő személyi állományát támogatva pénzügyi alapot hoztak létre. Továbbá szintén ebben az évben 16 kritikus területet állapítottak meg, ahol 2020-ra a NATO-erők fejlesztését tűzték ki célul. Ide sorolták a kibervédelmet is. A legnagyobb előrelépést azonban az jelentette, hogy a kibertámadást a NATO 5. cikkelye alá vonta, így egy virtuális térben történt támadásra a hagyományos értelemben vett harcászati tevékenységgel is reagálhatnak.[22]

Azonban 2016-os varsói NATO-csúcstalálkozó hozott a szövetség kiberbiztonsági politikájában gyökeres változást. A kiberteret a NATO kollektív védelmi feladatai közé sorolták, illetve a hadviselés egyik dimenziójaként ismerték el. A varsói NATO-csúcstalálkozón az Európai Tanács elnöke, az Európai Bizottság

---

18 Az Észak-atlanti Szerződés: Washington DC, 1949. április 4.

19 NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE

20 NATO Cyber Incident Response Capability, NCIRC

21 Cyber Threat Awareness Cell

22 CSIKI Tamás – TÁLAS Péter – VARGA Gergely: A NATO walesi csúcstalálkozójának napirendje és értékelése; Nemzet és Biztonság, 2014/4. pp. 112-128.

elnöke és a NATO főtitkára, egy EU és NATO közötti együttműködést írt alá, melynek célja a kooperáció még szorosabbá tétele a biztonság elérése érdekében.[23]

Egy évvel később, 2017-ben a miniszterek megegyeztek, hogy kiberképesség fejlesztését kezdeményezik a NATO missziókban és műveletekben.[24]

A NATO és az Európai Unió kiberbiztonsági együttműködése

A 2016-ban kiadott nyilatkozatban előrevetítették az együttműködést, amely során tovább támogatják a kutatást, technikai fejlesztést a kibervédelem területén. A reagálóképesség javítása érdekében párhuzamos és összehangolt kibervédelmi gyakorlatok rendezésére került sor egy hibrid forgatókönyvre reagálva 2017-ben a NATO, 2018-ban pedig az EU irányításával. 2017-ben Jens Stoltenberg, NATO főtitkár további tárgyalásokat folytatott az EU-NATO együttműködés fejlesztése érdekében. A találkozó során több területen is előrelépést tettek, többek között: a hibrid fenyegetések elleni küzdelem, információcsere, stratégiai kommunikáció és tengerpolitikai együttműködés tekintetében.

A 2018-as parlamenti ülésen az EP-képviselők kiemelték, hogy egyik szövetség sem rendelkezik olyan eszköztárral, amely teljes védelmet nyújtana az újfajta kihívással szemben. Azonban a kibertámadások száma növekszik a katonai és a civil fronton egyaránt, éppen ezért fontos a szövetségek szorosabb összefogása.

Urmas Paet észt EP-képviselő a következőket nyilatkozta a vele készített interjú során: *„Egy sikeres kibertámadás atombombát csinálhat az atomerőműből, vagy káoszt kelthet egy kórházban, veszélybe sodorva a betegek életét. A tagállamok, az EU és a NATO közti együttműködés fokozása révén meg kell erősítenünk kibervédelmi képességeinket ahhoz, hogy védekezni tudjunk az ilyen jellegű fenyegetések ellen.”*[25]

A képviselők úgy vélték, hogy a legnagyobb fenyegetést Kína, Észak-Korea és Oroszország jelenti. A NATO-EU szoros együttműködés mellett így egy gyors reagálású csoport létrehozását szorgalmazták, amely képes fellépni ezen támadások ellen.

Átütő változást a 2018-as brüsszeli csúcs jelentette, amelyen az EU-t képviselve részt vett Donald Tusk az Európai Tanács elnöke, Jean-Claude Juncker az Európai Bizottság elnöke és Federica Mogherini az Európai Unió külügyi és biztonságpolitikai főképviselője. Július 10-én aláírtak egy új, a közös együttműködésről szóló nyilatkozatot.[26]

---

[23] TÁLAS Péter: A varsói NATO-csúcs legfontosabb döntéseiről; Nemzet és Biztonság, 2016/2. pp. 97-101.

[24] PARÁDA István: A NATO kibervédelmi irányelvének fejlődése; Honvédségi Szemle 2018/3. pp. 3-12.

[25] http://www.europarl.europa.eu/hungary/hu/aktualis/2018-hirek/hirek-junius-2018/a-parlament-hathatosabb-kibervedelmet-a-nato-val-szorosabb-egyuttmukodest-akar.html (Letöltés ideje: 2018. 02. 05.)

[26] https://www.consilium.europa.eu/hu/policies/defence-security/defence-security-timeline/ (Letöltés ideje: 2018. 02. 05.)

Erről Donald Tusk a következőket nyilatkozta: *„A rendelkezésünkre álló valamennyi eszközt fel kívánjuk használni Európa polgárainak védelme érdekében, és ehhez nincs megfelelőbb partner, mint a NATO. Ezért állapodtunk meg a mai napon arról, hogy döntő fontosságú területeken megerősítjük az EU és a NATO közötti kapcsolatokat."*[27] Továbbá kiemelte, az EU-NATO együttműködés leginkább a terrorizmus, migráció, hibrid fenyegetések és kiberhadviselés elleni védelmet kívánja erősíteni.

Az Európai Unió kiberbiztonsági stratégiájának fejlődése

Biztonsági stratégia

A 2003 decemberében létrehozott „Biztonságos Európa egy jobb világban" elnevezésű biztonsági stratégia 2016-ig volt életben. Az évek során már nyilvánvalóvá vált, hogy ez a dokumentum nem tud reagálni Európa megváltozott biztonsági környezetére. Annak ellenére, hogy látható volt, hogy a stratégia túlzottan optimista, utópisztikus képet mutat, illetve a globális kihívásokra konkrét választ nem nyújt, a 2008-as felülvizsgálat során sem született új biztonsági stratégia.

2009-re már több tagország, köztük Olaszország, Lengyelország és Spanyolország is felismerte a tenger-, biztonság- és kiberstratégia hiányát, így sorra hoztak horizontális, illetve regionális kihívásokkal foglalkozó nemzeti stratégiákat. A 2003-as *Európai biztonsági stratégia* mégis egészen 2016-ig maradt életben. Ennek oka, hogy 2008-ban a gazdasági válság idején a kül- és biztonságpolitika helyett a pénzügyi-gazdasági kérdések kerültek a középpontba.

A változást a BREXIT-ről való népszavazás hozta meg. 2016 június 26-án Federica Mogherini[28] bejelentette, majd június 28.-án bemutatta a „Közös jövőkép, közös fellépés: erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája" című új globális biztonsági stratégiát.[29]

Kiberbiztonsági stratégia

2004. március 11-e nemcsak Spanyolország, hanem egész Európa számára megrázó dátum. Ezen a napon történt ugyanis a 191 halálos áldozatot követelő madridi terrortámadás, ami során tíz pokolgép robbant a spanyol főváros pályaudvarain. A terrortámadás során világossá vált, hogy Európa kritikus infrastruktúrája védtelen az ilyen jellegű támadásokkal szemben. Rávilágított emellett arra is, hogy az egyes szolgáltatások leállása egy egész állam megbénítását képes okozni.[30] A tragikus esemény következtében 2004 júniusában az Európa Tanács egy kritikus infrastruktúrák védelméről szóló stratégia kidolgozását kezdeményezte, melyet az Európai Közösségek Bizottsága októberben el is fogadott

---

[27] https://www.consilium.europa.eu/hu/meetings/international-summit/2018/07/11-12/ (Letöltés ideje: 2018. 02. 05.)

[28] az EU külügyi és biztonságpolitikai főképviselője

[29] MOLNÁR Anna: Az Európai Unió külkapcsolati rendszere és eszközei, Dialog Campus Kiadó 2018.

[30] https://hvg.hu/vilag/20140311_Percre_pontosan_tiz_eve_valt_pokolla_Madr (Letöltés ideje: 2018. 02. 05.)

„A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" címmel.

2005-ben fogadták el az úgynevezett EPCIP-et[31], ám ennek megvalósításáról 2008-ban született végleges döntés. Így jött létre „A kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint ezek védelmi fejlesztéseinek szükségességéről" szóló 2008/114/EK tanácsi irányelv.

Az irányelv megelőzésen, felkészülésen és ellenállóképességen alapszik. 2010-ben létrehozták a Digitális Menetrend nevű akciótervet, a számítógépes támadások elleni gyors reagálóképesség fejlesztése érdekében. Ennek keretein belül fogalmazták meg először a CERT[32] létrehozásának szükségességét. Még ebben az évben hozott rendeletet az Európai Tanács és Parlament az ENISA korszerűsítéséről és annak megerősítéséről, továbbá hozzájárult az ENISA, hogy az Európai Unió, annak tagállamai és az üzleti szféra szereplői szakszerűbben tudják kezelni a kibertérben történő esetleges támadásokat.[33]

Habár 2010-ben kiadtak egy „Öt lépés a biztonságosabb Európa felé" című dokumentumot, amely az informatikai hálózatok biztonságának növekedését tűzte ki célul, kiberbiztonsági stratégia nem született. Az Európai Unió azonban érezte ennek égető hiányát, így 2013-ra létrehozott egy két részből álló dokumentumot Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér címmel. Az első része az előzmények felvezetése után a kiberbiztonsági alapelveket tartalmazza.

Többek között kiemeli, hogy: *„Amiatt, hogy életünk minden területén egyre jobban függünk az információs és kommunikációs technológiáktól, olyan sebezhető pontok alakultak ki, amelyeket pontosan meg kell határozni, alaposan elemezni kell, meg kell oldani vagy mérsékelni kell. Minden érintett szereplőnek, köztük az állami szerveknek, a magánszektornak és az egyes polgároknak is el kell ismerniük ezt a közös felelősséget, fel kell lépniük a saját védelmükben, és szükség esetén összehangolt válaszlépéseket kell tenniük a kiberbiztonság erősítése érdekében."*[34]

A katonai és civil érintettség miatt az Európai Unió a NATO-val együttműködve kívánja a kibertámadásokkal szembeni ellenállóképességet fejleszteni. A NATO kiberbiztonsági stratégiájának az EU-ra gyakorolt további hatása és a két stratégia közötti összefüggés és együttműködés a publikációm egy előző fejezetében került részletes kifejtésre.

Az Európán belül egyre növekvő kiberbűnözés visszaszorítása érdekében a stratégia támogatja az EUROPOL szervezeteként létrejött az EUROPOL Kiberbűnözési Központot[35] (a továbbiakban: EC3), amely több területen látja el a kiberbűnözéssel kapcsolatos teendőket. Legfőbb feladatai közé tartozik a

---

31 European Programme for Critical Infrastructure Protection

32 Computer Emergency Response Team

33 PUSKÁS Béla: Az informatikai rendszerek és a jogi környezet változásai, Hírvillám, 2013/2. pp. 204-214.

34 https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex%3A52013JC0001 (Letöltés ideje: 2018. 02. 05.)

35 EC3: European Cyber Crime Center

kiberbűnözés elleni stratégia megalkotása, illetve az együttműködés a kiberbűncselekményekben eljáró hatóságokkal és a civil szférával is.[36]
„A számítástechnikai bűnözés elleni központot úgy alakították ki, hogy a nyomozásokhoz operatív és igazságügyi támogatást nyújtó központként kellő szakértelmet biztosítson, ugyanakkor képes legyen mozgósítani az uniós tagállamok valamennyi releváns erőforrását a számítástechnikai bűnözés jelentette fenyegetés enyhítése és korlátozása érdekében, függetlenül attól, hogy hol folytatják ezt a bűnöző tevékenységet."[37]

A Kiberbűnözési Központ három területen lát el feladatokat:

- kiber-cselekményekkel foglalkozó fókuszpont (FP Cyborg)
- gyermekek szexuális kizsákmányolásával foglalkozó fókuszpont (FP Twins)
- a bankkártyás csalásokkal foglalkozó fókuszpont (FP Terminal).[38]

NIS-irányelvek

A dokumentum második fele az úgynevezett NIS[39]*-irányelvekkel foglalkozik, melynek célkitűzése az európai infrastruktúra védelmének kiépítése. A cél eléréséhez szükséges, hogy a tagállamok rendelkezzenek egy nemzeti szintű stratégiával, amely biztosítja a hálózat- és információbiztonság magas szintjét, aminek következtében egy biztonságos és hatékony együttműködést épít ki az Európai Unió 28 tagállama*[40] *között. Fontos kiemelni továbbá, hogy a NIS nem egy általános érvényű szabályozás, hanem az alapvető szolgáltatást nyújtó szereplők (ivóvízellátók, energiacégek, banki szolgáltatók, közlekedési vállalatok) valamint a digitális szolgáltatók számára (online piacterek, keresőszolgáltatók) ír elő kötelezettségeket. Azt, hogy alapvető szolgáltatást nyújtó szereplők közé kik tartoznak, azt a tagállam saját maga dönti el az alapján, hogy az adott szereplő az ország gazdaságára, illetve társadalmára milyen hatással van.*[41] *Digitális szolgáltatók esetében azokra a szereplőkre is vonatkoznak a NIS-irányelvek, amelyek ugyan nem európai székhellyel bírnak, viszont itt is szolgáltatnak. Ennek értelmében például az amerikai Google-nek is meg kell felelni a NIS-irányelveknek, ha Európán belül is működni kíván. Biztosítania kell az IT-rendszereinek az alapvető biztonságát, továbbá a biztonságát érintő jelentős eseményeket köteles jelenteni a kijelölt szervezeteknek.*
Ugyan a NIS-irányelv már az EU 2013-as kiberbiztonsági stratégiájában is megjelenik, azonban csak a javaslat megszületése után 3 évvel, 2016 július 19.-én fogadták el. A tagországok 21 hónapos türelmi időt kaptak, mely során többek között ki kell jelölniük a NIS- irányelvek betartatására egy ezzel foglalkozó hatóságot. Egyik legfontosabb feladatuk pedig egy gyors reagálású kibervédelmi csapat kijelölése. Ezek az úgynevezett CERT-ek vagy CSIRT[42]*-ek.*[43]

---

36 KOVÁCS László: Kiberbiztonság és -stratégia; Dialóg Campus Kiadó, Budapest 2018b.
37 http://hevesmegye.hu/hu/europedirect/730-januar-11-en-megnyilik-a-szamitastechnikai-bnoezes-elleni-europai-koezpont (Letöltés ideje: 2018. 02. 05.)
38 KLIEN Tamás – SZABÓ Aliz – TÓTH András: Tanulmányok a tecnológia-és cyberjog néhány aktuális kérdéséről; Médiatudományi Intézet, Budapest 2018.
39 Network and Information Security – hálózat- és információbiztonság
40 A jelenlegi állás szerint 2019 március 29-től ez 27 tagállamra csökken, a BREXIT következtében.
41 KOVÁCS (2018b) i. m. 5.lj., pp. 254-247.
42 Computer Security Incident Response Team

2016-ban született meg az első, jogilag kötelező erejű kiberbiztonsági szabályrendszer az EU-ban. Ez az Európai Parlament és a Tanács 2016/1148 irányelve, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről című dokumentum.

Egy évvel később az Unió kiberbiztonságának megerősítése tovább folytatódott. Jean-Claude Juncker az Európai Bizottság elnöke a következőképp nyilatkozott 2017. szeptember 19.-én az Európai Unió kiberbiztonsági helyzetéről: „Az elmúlt három évben előrelépéseket tettünk az európaiak online biztonságának garantálása terén. Ám Európa még mindig nem rendelkezik elég eszközzel a kibertámadások elhárítására. A Bizottság ezért ma új eszközöket javasol az ilyen támadásokkal szembeni védelem megerősítésére, többek között egy európai kiberbiztonsági ügynökség létrehozását."[44]

Az Európai Bizottság a külügyi és biztonságpolitikai főképviselővel egy olyan javaslatcsomagot dolgoztak ki 2017-ben, amely nagymértékben növeli az Európai Unió kibertámadásokkal szembeni reagálóképességét. A javaslatban szerepel többek között, hogy szükség van egy ENISA-ra épülő Európai Uniós Kiberbiztonsági Ügynökség felállítására, amely a tagállamok számára segítséget nyújt a számítógépes támadások kivédésére, illetve azok kezelésére. Továbbá az Ügynökség az EU és tagállamai felkészültségét egy évente megrendezésre kerülő páneurópai kiberbiztonsági gyakorlattal kívánja javítani.[45]

Az Európai Unió kiberbiztonsága napjainkban

A 2018 októberében történő Európai Tanács ülésén a BREXIT, migráció, illetve a globális felmelegedés okozta kihívások mellett újra középpontba került a belső biztonság kérdése, ezen belül is a legfőbb kihívásnak a kiberhadviselést minősítették az áprilisi eseményekre reagálva. 2018 áprilisában ugyanis a hágai székhelyű Vegyifegyver-tilalmi Szervezet (továbbiakban OPCW) ellen az orosz katonai hírszerző szolgálat kibertámadást hajtott végre. Habár az akció a holland hírszerző szolgálatok, illetve az Egyesült Királyság fellépésének köszönhetően meghiúsult, ismételten felhívta az EU figyelmét, hogy tagállamai és intézményei ellenálló képességét a digitális területen még inkább meg kell erősítenie.[46]

A kiberbiztonság kiépítésének legnagyobb kihívása a folyamatosan változó és fejlődő technikai újítások, mellyel a biztonság területe nem tudja felvenni a versenyt. Ennek javítása érdekében hozták létre a nemzeti koordinációs központok hálózatát, amely a kutatásra és fejlesztésre fennálló finanszírozást koordinálja, teszi célzottabbá. 2018 decemberében az EU tagállamainak állandó képviselői elfogadtak egy, az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló jogszabályt, amely során lehetővé válik a csatlakozó

---

43 Mára a két mozaikszó szinonimává vált Az EU a CSIRT-et, míg Magyarország inkább a CERT-et használja.

44 http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (Letöltés ideje: 2018. 02. 05.)

45 https://www.consilium.europa.eu/hu/policies/cyber-security/ (Letöltés ideje: 2018. 02. 05.)

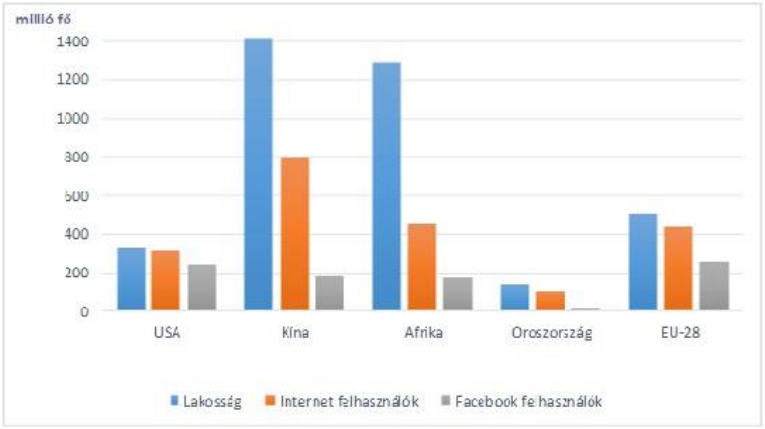
46 https://www.consilium.europa.eu/hu/policies/tallinn-leaders-agenda (Letöltés ideje: 2018. 02. 05.)

információs, kommunikációs eszközök és szolgáltatások kiberbiztonsági tanúsítása az összes tagország számára. Ezzel kívánják a felhasználók bizalmát megnyerni, illetve a vállalkozásokat az EU-n kívüli üzleti befektetésekre is ösztönözni.[47]

Jövőkép

A média egyre nagyobb befolyással bír a politika alakulására. Előszeretettel használja ezt Oroszország és Kína is, aki az egyik legnagyobb veszélyt jelenti mind az EU-ra mind a NATO-ra nézve. Az, hogy Oroszország hatalmas médiabefolyással rendelkezik Kelet-Európában, már eddig is nyilvánvaló volt, ám a 2016-os amerikai, vagy az azt követő francia választások alatt történő kibertámadások bebizonyították, hogy az orosz befolyás a balti államokon túl is elér. A támadások célpontja a kormányzati intézmények, kritikus infrastruktúrák és politikához köthető vállalatok voltak.[48] Egyre nagyobb befolyással bír a Russia Today (továbbiakban RT) című orosz, állami finanszírozású televíziós csatorna, amely külföldi nézőit kívánja megnyerni országa jóhírének növelése érdekében, az információk eltorzításával. 2017-ben az amerikai Szövetségi Nyomozó Iroda, azaz az FBI nyomozást indított az orosz csatorna ellen, ugyanis azt gyanították, hogy befolyásolták az amerikai elnökválasztást. A szakértők az RT további térnyerését jósolják, így az Európai Uniónak és a NATO-nak a jövőben fel kell készítenie tagországait az orosz médiabefolyás ellen.

Az egész világban nagy befolyással bír a közösségi médiák, leginkább a Facebook térnyerése. 2017-es statisztika alapján 1,8 milliárd aktív felhasználóval rendelkezett a Facebook. Az európai általános adatvédelmi rendelet (GDPR) elfogadásával, a felhasználók önként hagyják jóvá műveleteinek, beszélgetéseinek rögzítését, de még a tartózkodási helyet is nyomon tudja követni.[49]



1. ábra Az internetfelhasználók megoszlása a Facebook felhasználókkal összevetve
Forrás: https://www.internetworldstats.com/stats1.htm (Letöltés ideje: 2018. 02. 05.)

[47] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2018:0630:FIN:HU:PDF (Letöltés ideje: 2018. 02. 05.)
[48] KOVÁCS (2018b) i. m. 5.lj, pp. 115-119.
[49] KOVÁCS (2018b) i. m. 5. lj, pp. 76-80.

Az Internet World Stats 2017-es, illetve 2018-as adatai alapján készített diagrammokon látható az internet, illetve a legnépszerűbb közösségi média felhasználóinak nagyarányú száma.[50] Az ábrán látható adatok szerint Kína és Oroszország lakossága számához képest a Facebook felhasználók száma elenyésző. Ennek az az oka, hogy Kína blokkolja mind a Google, mind a Facebook szolgáltatását. Oroszország már évek óta törekszik arra, hogy az internetes forgalom az országon kívül maradjon. A 2018-ban készült törvénytervezet alapján egy külföldről érkező kibertámadás esetén a helyi netszolgáltatók kötelesek lecsatlakozni a globális világhálóról, ezzel védve meg az országot a csapással szemben. Fontos azonban azt is kiemelni, hogy a törvényjavaslat elfogadása esetén Oroszország nem csak a kiberbiztonságát erősítené meg, hanem növelné a kiber-támadóképességét is. Ezek alapján elmondhatjuk, hogy az Európai Uniónak és a NATO-nak a jövőben olyan mértékben kell kiépítenie a kibertámadásokra való reagálóképességét, hogy egy esetleges orosz vagy kínai támadás ellen is védelmet biztosítson.

Annak érdekében, hogy a NATO védelmet nyújtson a tagállamai számára egy esteleges kibertámadás során, a már említett walesi NATO csúcson kijelentették, hogy a kibertámadás a NATO 5. cikk hatálya alá tartozik, így a szövetség jogilag válaszlépésre jogosult tagországai védelme érdekében. Szenes Zoltán tanulmányában mégis kételyekkel él ezzel szemben és számos kérdést vet fel.[51]
„Philip Breedlove tábornok, európai főparancsnok augusztusban már nyilatkozott arról, hogy a tagországok területére felségjelzés nélkül behatoló erők (sajtónevükön: „little green men") tevékenysége ugyanúgy a szövetség 5. cikkének hatálya alá tartozik, mint a hagyományos támadás, nehéz megítélni, hogy a beszivárgás mikor éri el a NATO-erők bevetéséhez szükséges küszöbértéket. Hasonló a helyzet a kiberfenyegetésekkel is. Hiába döntött a NATO most arról, hogy egy ország ellen indított kibertámadást (ilyen eset 2007-ben történt, Észtország ellen) az 5. cikk hatálya alá tartozónak tekint, kétséges, hogy pontosan meg lehet-e állapítani, hogy ki és honnan támadott. Egy téves reakció pedig beláthatatlan politikai, diplomáciai és katonai következményekkel járhat. Nem beszélve arról, hogy az 5. cikk aktivizálásához teljes konszenzusra van szükség, vagyis valamennyi országnak egyformán kell megítélnie a helyzetet."[52]

Összefoglalás

Tanulmányomban látható, hogy a technológia gyors fejlődése milyen hatással van az Európai Unióra és a NATO-ra. A kibertér egyre növekvő szerepe okán a kibervédelem új globális kihívásként jelenik meg. Ez az újfajta dimenzió hatással van az egész világra. Nincsenek a klasszikus értelemben vett határok, az esetleges támadásokat térben és időben is nehéz meghatározni. Az Európai Unió több esetben a NATO-ban sikeresen alkalmazott megoldásokhoz nyúl, de önálló szervezeteket is létrehoz, illetve folyamatokat szabályoz le annak érdekében, hogy egy kontrollált környezetben működjenek a kibertérben lezajló események. A NATO-nak és az EU-nak fel kell készülnie a technológia további fejlődésére, a hibrid hadviselés erősödésére a tagállamok digitalizálódásának folytatására. Számolni kell továbbá

[50] https://www.internetworldstats.com/stats1.htm (Letöltés ideje: 2018. 02. 05.)
[51] SZENES Zoltán: Új bor a régi palackban? A walesi NATO csúcs; Hadtudomány, 2014/3-4. pp. 3-21.
[52] SZENES i. m. 46. lj p. 16.

azzal is, hogy a fiatalabb generáció egyre inkább az infokommunikációs eszközöktől és az internettől függenek. Az Eurostat 2017-ben készített statisztikája szerint az európai polgárok több mint 84%-a rendszeresen használja az internetet.[53] Az adatok szerint a lakosság több mint 72%-a napi, még további 8%-a heti rendszerességgel lépett fel a világhálóra. Ezzel szemben mégis megdöbbentő az a statisztika, ami azt elemzi, milyen arányban korlátozták a személyes adataikhoz való hozzáférést a polgárok 2016-ban. Az Európai Unió 28 tagállama internetfelhasználóinak csupán 28%-a nem adott meg semmilyen személyes adatot az interneten.[54]

Ezen adatokból látható, hogy bár az uniós polgárok túlnyomó részének mindennapi életévé vált az internethasználat, a személyes adataik védelméért kevesen tesznek, holott az információs biztonság mind a tagállamok mind azok állampolgárai közös érdeke. A fejlett technológia és az állam digitalizálásnak köszönhetően a kibertér fenyegetettsége mindenkit érintő problémává vált: *„…az európai számítógépes infrastruktúra igen fejlett, a számítógépes hálózatok valamennyi szektort átszövik, az azokon tárolt adatok köre és mennyisége fokozatosan növekszik, mindez pedig vonzó terepet kínál a számítógépes bűnözőknek. Ezért egyre fontosabbá és sürgetőbbé válik egy összehangolt, komplex európai szabályrendszer megalkotása…"*[55]

Az Európai Uniónak a NATO-val együttműködve kell megkeresni a helyes válaszokat a kihívásokra, melyeket a NATO szövetségeseivel, illetve az Európai Unió tagállamaival kell a gyakorlatba is átültetni.

Felhasznált irodalom:

- A hálózati és információs rendszerek biztonságára vonatkozó Stratégia, http://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf, p. 3. (Letöltés ideje: 2018. 02. 05.)
- CSIKI Tamás – TÁLAS Péter – VARGA Gergely: A NATO walesi csúcstalálkozójának napirendje és értékelése; Nemzet és Biztonság, 2014/4. pp. 112-128.
- Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52005DC0576&from=EN (Letöltés ideje: 2018. 02. 05.)

[53] A felmérést 3 hónapon keresztül végezték a 16-74 év közötti európai uniós állampolgárokon.

[54] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Information_society_statistics/hu&oldid=86122; (Letöltés ideje: 2018. 02. 05.)

[55] MOLNÁR Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése; Hadmérnök, 2017/1. pp. 255-267.

- KLIEN Tamás – SZABÓ Aliz – TÓTH András: Tanulmányok a tecnológia-és cyberjog néhány aktuális kérdéséről; Médiatudományi Intézet, Budapest 2018.
- KOVÁCS László: A kibertér védelme; Budapest, Dialóg Campus Kiadó 2018a. p. 18.
- KOVÁCS László: Kiberbiztonság és -stratégia; Dialóg Campus Kiadó, Budapest 2018b.
- MAGYAR Sándor – SIMON László: A terrorizmus és indirekt hadviselése az EU kiberterében, Szakmai Szemle: 2017/4. p. 65.
- MOLNÁR Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése; Hadmérnök, 2017/1. pp. 255-267.
- MOLNÁR Anna: Az Európai Unió külkapcsolati rendszere és eszközei, Dialog Campus Kiadó 2018.
- MUNK Sándor: A kibertér fogalmának egyes, az egységes értelmezését biztosító kérdései; Haditechnika, 2018/1. p. 115.
- MUNK Sándor: Információbiztonság vs informatikai biztonság; Hadmérnök, 2007/különszám p. 12.
- PARÁDA István: A NATO kibervédelmi irányelvének fejlődése; Honvédségi Szemle 2018/3. pp. 3-12.
- PUSKÁS Béla: Az informatikai rendszerek és a jogi környezet változásai, Hírvillám, 2013/2. pp. 204-214.
- PUSKÁS Béla: A diplomácia és a virtuális tér kapcsolata; Felderítő Szemle 2018/3. pp. 39-55.
- RESPERGER István: A válságkezelés és a hibrid hadviselés; Budapest, Dialog Campus 2018. p. 21.
- RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban; Budapest, Zrínyi Kiadó 2014. p. 23.
- SZENES Zoltán: Új bor a régi palackban? A walesi NATO csúcs; Hadtudomány, 2014/3-4. pp. 3-21.
- TÁLAS Péter: A varsói NATO-csúcs legfontosabb döntéseiről; Nemzet és Biztonság, 2016/2. pp. 97-101.
- ÜRMÖSI Károly: A biztonság, a biztonság fogalma; Hadtudományi Szemle, 2013/4. p. 148.
- VARGA Péter János: A kritikus információs infrastruktúrák értelmezése; Hadmérnök, 2008/3. pp. 149-156.
- https://www.citatum.hu/szerzo/Eric_Emerson_Schmidt (Letöltés ideje: 2018. 02. 05.)
- https://www.consilium.europa.eu/hu/policies/defence-security/defence-security-timeline/ (Letöltés ideje: 2018. 02. 05.)

- https://www.consilium.europa.eu/hu/meetings/international-summit/2018/07/11-12/ (Letöltés ideje: 2018. 02. 05.)
- http://www.europarl.europa.eu/hungary/hu/aktualis/2018-hirek/hirek-junius-2018/a-parlament-hathatosabb-kibervedelmet-a-nato-val-szorosabb-egyuttmukodest-akar.html (Letöltés ideje: 2018. 02. 05.)
- https://hvg.hu/vilag/20140311_Percre_pontosan_tiz_eve_valt_pokolla_Madr (Letöltés ideje: 2018. 02. 05.)
- http://hevesmegye.hu/hu/europedirect/730-januar-11-en-megnyilik-a-szamitastechnikai-bnoezes-elleni-europai-koezpont; (Letöltés ideje: 2018. 02. 05.)
- http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (Letöltés ideje: 2018. 02. 05.)
- https://www.consilium.europa.eu/hu/policies/cyber-security/ (Letöltés ideje: 2018. 02. 05.)
- https://www.consilium.europa.eu/hu/policies/tallinn-leaders-agenda (Letöltés ideje: 2018. 02. 05.)
- https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2018:0630:FIN:HU:PDF (Letöltés ideje: 2018. 02. 05.)
- https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex%3A52013JC0001 (Letöltés ideje: 2018. 02. 05.)
- https://www.internetworldstats.com/stats1.htm (Letöltés ideje: 2018. 02. 05.)
- https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Information_society_statistics/hu&oldid=86122; (Letöltés ideje: 2018. 02. 05.)

E SZÁMUNK TARTALMA

CONTENTS

FELEGYI JÚLIA

NEMZETKÖZI GYAKORLAT A MENEDÉKKÉRŐK SZEXUÁLIS IRÁNYULTSÁGÁNAK VIZSGÁLATA KÖRÉBEN

Írásomban azon menedékkérők meghallgatásával foglalkozom, melyek LGBTI-csoporthoz való tartozásukat jelölték meg menekülésük okaként. A szenzitív kérdéskört nemzetközi szinten vizsgálva kerestem információkat a különböző országok gyakorlatáról és szabályozásáról. A szükséges fogalomtisztázásokat követően elsőként hazánk gyakorlatát és lehetőségeit mutatom be, és egy 2018-as, vélhetően precedens értékű ítéletet részletezek. Ezt követően az Egyesült Királyság és az Amerikai Egyesült Államok gyakorlatát mutatom be, végül az Európai Unió tagországainak relevánsabb és aktuálisabb eszközrendszerét szemléltetem. Összegzésemben javaslatokat is megfogalmazok a hatékonyabb ítélethozatalt elősegítendő.

Kulcsszavak: migráció, menekültügyi meghallgatás, homoszexuális menedékkérő

DR. RÉPÁSI KRISZTIÁN

AZ EURÓPAI UNIÓ LAKOSAINAK TERRORIZMUSSAL KAPCSOLATOS FENYEGETETTSÉG-PERCEPCIÓJA 2012 TAVASZA ÉS 2018 TAVASZA KÖZÖTT

Az Európai Unió lakosságának terrorizmussal kapcsolatos fenyegetettség-percepcióját azért fontos elemezni, mert a vizsgálat képet ad arról, hogy az EU polgárai mennyire tartják fontosnak a terrorizmus problémáját. 2012 tavasza és 2015 tavasza között a válaszadók nem gondolták azt, hogy a terrorizmus a legnagyobb problémák közé tartozna, ugyanis a mindennapi élettel kapcsolatos nehézségek fontosabbak voltak a terrorizmusnál. 2015-öt követően viszont érezhetően nőtt a terrorizmustól való félelem, ami elsősorban az uniós szintű, kisebb részben pedig a nemzeti szintű problémák értékelésénél jelent meg. Ennek oka, hogy az európai közvélemény vélhetően összekapcsolta a vallási indíttatású merényleteket a menekültekkel és a bevándorlókkal.

Kulcsszavak: fenyegetettség-percepció, Eurobarometer, terrorizmus, Európai Unió, migráció

JÚLIA FELEGYI

INTERNATIONAL PRACTICE IN EXAMINING THE SEXUAL ORIENTATION OF ASYLUM SEEKERS

In my writing, I deal with the listening of the asylum seekers who have identified their affiliation with the LGBTI group as the cause of their escape. Looking at the sensitive issue at international level, I sought information on the practices and regulations of different countries. Following the necessary clarifications, first I introduce the practice and possibilities of our country and details of a verdict of 2018, what will be presumably a precedent. Then I will describe the practice of the United Kingdom and the United States and, finally, I will present a more relevant and up-to-date toolbox for the member states of the European Union. In my summary, I make proposals for more effective judgments.

Keywords: migration, homosexual asylum-seeker, LGBTI-interview

KRISZTIÁN RÉPÁSI DR.

THE TERRORISM THREAT PERCEPTION OF EU CITIZENS BETWEEN SPRING 2012 AND SPRING 2018

Analysis of the EU citizens' terror threat perception is quite important because the examination gives an idea of how the EU citizens consider terrorism as a problem. EU citizens did not consider terrorism as the most important problem between spring 2012 and spring 2015 because everyday problems were more important to them than terrorism. At the same time, terror threat perception has noticeably risen since 2015. The increase of threat perception has appeared primarily in the evaluation of problems at EU level and, to a lesser extent, at national level. The possible reason for the high terrorism threat perception was that EU citizens linked religiously inspired incidents to the migrants and refugee seekers.

Keywords: threat perception, Eurobarometer, terrorism, European Union, migration

KOÓS GÁBOR – PROF. DR. SZTERNÁK GYÖRGY

A SZÍRIAI POLGÁRHÁBORÚ GEOPOLITIKAI, GEOSTRATÉGIAI HÁTTERE, AZ OROSZ KATONAI MŰVELETEK JELLEMZŐI

„Sok országban furcsa határok vannak” – mondja Rami George Khouri, a Bejrútban működő Amerikai Egyetem Közpolitikai és Nemzetközi Ügyek Intézetének volt igazgatója. „Az arabok számára Sykes-Picot-egyezmény a legmélyebb sérelem szimbóluma. Egy egész század telt el, amelyben a nyugati hatalmak velünk játszottak és katonailag is támadtak minket.”

Kulcsszavak: szíriai polgárháború, geopolitikai és geostratégiai háttér, Iszlám Állam, orosz katonai műveletek, Geraszimov vezérkari főnök interjúja

DR. ANDREIDES GÁBOR

A TERRORIZMUS HATÁSA ÉS KEZELÉSE OLASZORSZÁGBAN AZ „ÓLOMÉVEK” ALATT

Beszédes névvel illeti a szakirodalom és az köznyelv Olaszország hetvenes éveit. „Anni di piombo” – vagyis ólomévek. Az ország a jobboldali és a baloldali terror csapásai alatt állott, az állam súlyos csapásokat szenvedett. Az évtized hagyományosan - és ez a megállapítás tulajdonképpen helytálló – legsúlyosabb terrorcselekményének a kereszténydemokrata Aldo Moro elrablását, ötvenöt napos fogságát és kivégzését tartjuk. A Vörös Brigádok (Brigate Rosse) szélsőbaloldali terrorszervezet 1978. március 16-án rabolta el a képviselőt, aki éppen pártársának, a szintén kereszténydemokrata Giulio Andreotti kormányának bizalmi szavazására igyekezett. Az ötvenöt napi fogság alatt számos politikus, közéleti személy, sőt még VI Pál pápa is szót emelt Moro szabadon bocsájtása mellett. Erőfeszítéseiket nem koronázta siker: a kereszténydemokrata politikus holtestét május 9-én találták meg Róma egyik utcájában, egy autó csomagtartójába rejtve félúton a Kereszténydemokrata Párt (Democrazia Cristiana) és az Olasz Kommunista Párt (Partito Comunista Italiano) székháza között.

Kulcsszavak: szélsőbal, szélsőjobb, állam, olasz állam, terror, Aldo Moro, Giulio Andreotti, Vörös Brigádok

GÁBOR KOÓS – GYÖRGY SZTERNÁK PROF. DR.

THE GEOPOLITICAL AND GEOSTRATEGIC BACKGROUND OF THE CIVIL WAR IN SYRIA, THE FEATURES OF THE RUSSIAN MILITARY OPERATIONS

"Lots of countries have strange borders," says Rami George Khouri of the American University of Beirut. "Yet for Arabs, the Sykes-Picot agreement is a symbol of a much deeper grievance against colonial tradition. there was a whole century when Western powers have played with us and were involved militarily."

Keywords: Syrian civil war, geopolitical and geostrategic background, Islamic State, Russian military operations, chief of staff general Gerasimov interview

GÁBOR ANDREIDES DR.

THE EFFECTS OF TERRORISM AND THEIR HANDLING DURING "THE LEAD YEARS" IN ITALY

In Italy, scholars and other people use a very characteristic term to describe the 1970s. 'Anni di piombo' – i.e. 'Years of Lead'. State and society suffered from the terror coming both from the Right and the Left. The kidnapping, capture (lasting 55 days) and execution is considered the most severe terrorist act, which we can approve nowadays, too. The extremely leftist organisation of the Red Brigades (Brigate Rosse) kidnapped the politician on 16 May, 1978 when he was on his way to give his vote of confidance in favour of his fellow member of the Christian Democratic Party, Giulio Andreotti. During his capture, many politicians, public figures, even Pope Paul VI made efforts to convince the terrorist of releasing Moro. Their voices remained unheard: the christian democratic politician's body was found on 9 May in a trunk of a car midway between the headquarters of the Christian Democratic (Democrazia Cristiana) and the Communist (Partito Communista Italiano) parties.

Keywords: extreme left, extreme right, state, Italian state, terror, Aldo Moro, Giulio Andreotti, Red Brigades

TÓTH TAMÁS

AZ EURÓPAI UNIÓ TERVEZETT KIBERBIZTONSÁGI TANÚSÍTÁSI KERETRENDSZERÉNEK BEMUTATÁSA

A publikáció az Európai Bizottság SWD(2017) 500 final számú hatásvizsgálatának IKT (információs és kommunikációs technológia) tanúsítási területét hivatott összefoglalni magyar nyelven, mivel a teljes dokumentáció csak angol nyelven jelent meg. A dokumentáció kiemelt jelentőségű területet vizsgál az IKT termékek kiberbiztonsági tanúsításának tükrében. Az EU-s jogalkotók 2018 decemberében politikai nyilatkozatot adtak ki a „Kiberbiztonsági jogszabály”-ról, melyben meghatározásra kerül az EU kiberbiztonsági tanúsítási keretrendszerének kidolgozása.
Az Európai Bizottság az európai IKT piac optimális növekedésének, biztonságának érdekében szakpolitikai intézkedési javaslatokat dolgozott ki a hatásvizsgálatban, melyek közül az elfogadott javaslat képezi az uniós szintű IKT tanúsítási keretrendszer alapjait. A cikk fő célja e keretrendszer kialakításának, jellemzőinek és hatásainak vizsgálata, továbbá a Magyarország számára származó előnyök ismertetése.

Kulcsszavak: Európai kiberbiztonsági tanúsítási keretrendszer, digitális egységes piac, dolgok internete, kiberbiztonság

DR. KASSAI KÁROLY

KIBERTÉR – AKTUÁLIS VÁLTOZÁSOK

A kibertérre vonatkozó nemzeti és nemzetközi szempontok civil és katonai nézőpontból egyaránt évről-évre egyre bonyolultabbá válnak. A fenyegetések bonyolultsága és hatásaiknak növekedése, a megjelenő kritikus sérülékenységek, a halmozódó negatív hatások a védelmi rendszabályok folyamatos fejlesztését igénylik. A katonai szempontok ezen túlmenően tartalmazzák a katonai műveletek teljes spektrumú támogatását, beleértve a kibertérben kifejtett hatásokat is.
A publikáció a kibertérrel kapcsolatos fontosabb nemzetközi és nemzeti változásokat mutatja be. A legfontosabb nemzeti változás, hogy Magyarországon a kibertér is katonai műveleti terület - hasonlóan a NATO és EU nézőponthoz.

Kulcsszavak: kibertér, kibertér-művelet, biztonsági követelmény, kiberfenyegetés, műveleti terület.

TAMÁS TÓTH

PRESENTATION OF THE PLANNED FRAMEWORK FOR EUROPEAN CYBERSECURITY CERTIFICATES

This research aims to summarize in Hungarian language the findings of the European Commission's No. SWD(2017) 500 final Impact Assessment regarding ICT certification, since the entire document has only been published in English language so far. The document examines an outstandingly important area regarding ICT products' cybersecurity certification. In December 2018 EU lawmakers issued a political agreement on the „Cybersecurity Act", laying down the fundament for the development of a framework for European Cybersecurity Certificates.
To ensure the optimal growth and security of the European ICT market, the European Commission came up with policy recommendations in its Impact Assessment, of which the accepted recommendation forms the basis of the EU-level ICT certification framework. The aim of this research is to examine the formation, characteristics, and impact of the above mentioned framework, and to point to its benefits to Hungary.

Keywords: Framework for European Cybersecurity Certificates, Digital Single Market, Internet of Things, cyber security

KÁROLY KASSAI DR.

CYBER SPACE – ACTUAL CHANGES

National and international aspects of cyberspace are becoming increasingly complex from civil and military point of view year by year. The complexity of threats and the increase in their impact, the critical vulnerabilities and the aggregation of negative effects emerging require the continuous development of security regulations. In addition, military aspects include full support of military operations, including cyber effects.
The article presents main international and national changes in cyberspace. The most important national change is that the cyber space in Hungary is also military operation area - similar to the NATO and EU perspective.

Keywords: cyberspace, cyberspace operations, security requirement, cyber threat, operation domain.

BEDERNA ZSOLT

BIZALOM ÉS MEGBÍZHATÓSÁG

A magánéletben, a gazdaságban, a politikában az egyén, a vállalat és a közösség különböző szintjein az egyes entitások együttműködésének alapja a bizalom, ennél fogva annak egy megkerülhetetlen tényezője, összetevője. A bizalom egy objektív tényekből és szubjektív érzetből összetevődő paramétert takar, amellyel az egyik entitás a másik felet felruházza. E paraméter értékének növelése, azaz a minél magasabb bizalmi szint kialakítása a mindennapi tapasztalatok szerint többnyire hosszú idő alatt végbemenő folyamat eredménye, azonban elveszítése pillanatok kérdése lehet. Célom a bizalom és azzal összefüggésben a bizalom és megbízhatóság kérdéskörének vizsgálata az információbiztonság három aspektusa közül a logikai és az adminisztratív síkjának vonatkozásában.

Kulcsszavak: bizalom, megbízhatóság, BMIS modell

HASILLÓ GYÖRGY

BEMUTATKOZIK A GÁZOLÁSOS TERRORCSELEKMÉNYT MEGAKADÁLYOZÓ VÉDELMI RENDSZER (GTMVR)

A tanulmány a gázolásos terrorcselekményt megakadályozó védelmi rendszer (GTMVR) elméletét vázolja fel, egy olyan komplex szisztémát, amely a közterületek autóktól elválasztott területeit hivatott megvédeni a gépjárműves támadásokkal szemben. Öt fő komponense: a járdákba épített rejtett, avagy süllyesztett oszlopok, az ezeket és a különböző szenzorokat is vezérlő mesterséges intelligencia, a támadó személyek ellen fellépő drónok, az egész rendszer mögött álló, folyamatosan bővülő adatbázis, valamint a kisegítő eszközök, úgymint kamerák, érzékelők, internethálózat. A dokumentum elméleti síkon vázolja a rendszer bemutatását, annak elemeit, működését. Írásának célja, hogy még ha csak elméleti szinten is, de segítséget nyújtson a rendvédelmi szervek jövőbeli tevékenységéhez, az alja, gonosz szándékból elkövetett merényletek megakadályozásában, melyek ártatlan emberéleteket veszélyeztetnek szerte a világon.

Kulcsszavak: GTMVR, gázolásos terrorcselekmény, komplex védelmi rendszer

PUSKÁS ADRIENN

A NATO ÉS EU KIBERVÉDELMI POLITIKÁJÁNAK ÁTTEKINTÉSE

Az informatika terén végbemenő változások új kihívások elé állítják a nemzetek biztonságát. Jelen írás a NATO és EU kiberbiztonsági stratégiáját és politikáját tekinti át és röviden ismerteti a hálózatbiztonsági irányelvet. A tanulmány felvázolja, hogy az elmúlt évtizedben az Európai Unió milyen lépéseket tett a kiberbiztonsági szabályrendszer és az egységes európai digitális piac megteremtése terén.

Kulcsszavak: kritikus infrastruktúra, kibervédelem, információbiztonság, NATO, EU

ZSOLT BEDERNA

TRUST AND TRUSTWORTHINESS

In various level of private life, the economy and the politics, the cooperation of entities is based on trust, which has objective and subjective components. It is a basic parameter created by the entrusting entity for each entrusted one. Increasing this parameter to reach A higher and higher value is a long process, but, due to experiences, it may take seconds to lose its value. My goal is to inspect trust and trustworthiness in the aspect of logical and administrative security.

Keywords: trust, trustworthiness, BMIS model

GYÖRGY HASILLÓ

INTRODUCING THE VRAPS – THE SYSTEM DEEMED TO PREVENT RAMMING TERRORIST ACTS

The study outlines the theory behind VRTPS aka Vehicle Ramming Attack Prevention System which is a complex method destined for protecting public places separated from traffic against vehicle ramming-type terror threats. It has five major components: the hidden security bollards built into sidewalks, the artifical intelligence controlling these and different sensors and detectors, the drones that can take action against suspects, the database behind the whole system as well as the subsidiary tools just like cams, sensors and internet.

This essay features the introduction of the system academically, it shows its components and their functions. The aim of this writing is that to give help to law enforcement agencies for their future activity against outragest hat come from despicable and evil intentions and riskong innocent lives around the globe.

Keywords: VRAPS, Vehicle Ramming, complex prevention system

ADRIENN PUSKÁS

REVIEW OF NATO AND EU CYBER DEFENCE POLICIES

Changes in the information technology are generated new challenges in the security of nations. This present paper analyses NATO and EU cyber security strategy and policy and briefly describes the NIS directive. The study outlines what steps the European Union has taken in the creation of regulations in the past decade.

Keywords: critical infrastructure, cyber security, information security, NATO, EU

SZERZŐINK

Dr. Andreides Gábor	PhD, ELTE Történelemtudományi Doktori Iskola, oktató
Bederna Zsolt	Óbudai Egyetem Biztonságtudományi Doktori Iskola, doktorandusz hallgató
Dr. Boda Mihály	PhD, NKE HHK, Hadtörténelmi, Filozófiai és Kultúrtörténeti Tanszék, mb. tanszékvezető, egyetemi docens
Felegyi Júlia	NKE Hadtudományi Doktori Iskola, doktorandusz hallgató
Hasilló György	Óbudai Egyetem Dékáni Hivatal munkatársa
Dr. Kassai Károly	ezredes, PhD, a KNBSZ munkatársa
Koós Gábor	nyá. alezredes
Puskás Adrienn	NKE Nemzetközi és Európai Tanulmányok Kar, BSC hallgató
Dr. Répási Krisztián	PhD, NKE Stratégiai Védelmi Kutatóközpont, külső munkatárs
Prof. Dr. Szternák György	nyá. ezredes, CSc, NKE egyetemi tanár
Szűcs László	őrnagy, a KNBSZ munkatársa
Tóth Tamás	NKE MSC hallgató

E SZÁMUNKAT LEKTORÁLTÁK

Görbe Attiláné Dr. Zán Krisztina	r. ezredes, NKE Tudományos Ügyek Iroda, irodavezető
Dr. Háry Szabolcs	ezredes, PhD, a KNBSZ munkatársa
Dr. Kassai Károly	ezredes, PhD, a KNBSZ munkatársa
Dr. Kenedli Tamás	ezredes, PhD, a KNBSZ munkatársa
Dr. Kis-Benedek József	nyá. ezredes, PhD, NKE, c. egyetemi tanár
Dr. Kovács Tamás	PhD, NKE RTK, Rendészeti Vezetéstudományi Tanszék, egyetemi docens
Dr. Magyar Sándor	ezredes, PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék, adjunktus, a KNBSZ munkatársa
Dr. Puskás Béla	alezredes, PhD, a KNBSZ munkatársa
Prof. Dr. Rajnai Zoltán	PhD, Óbudai Egyetem Biztonságtudományi Doktori Iskola vezetője
Tóth Csaba Mihály	alezredes, a KNBSZ munkatársa
Dr. Tömösváry Zsigmond	ny. dandártábornok, PhD, a Felderítők Társasága Egyesület elnöke

A SZAKMAI SZEMLÉBEN TÖRTÉNŐ PUBLIKÁLÁS FELTÉTELEI

Az írásművekkel szemben támasztott követelmények

Etikai követelmények:

- az írásmű máshol, ebben a formájában még nem jelent meg;
- a szerző(k) kizárólagos szellemi tulajdona, melyet szerzői nyilatkozat aláírásával igazol(nak);
- korrekt, visszakereshető hivatkozásokkal ellátott;
- bibliográfiával ellátott (amely tartalmazza a hivatkozott irodalom jegyzékét, az internetes anyagok jegyzékét a letöltés idejével együtt);
- a szerző(k) saját véleményét is tükrözheti, mely értelemszerűen nem mindig egyezik meg a Szolgálat álláspontjával.

Tartalmi követelmények:

- a folyóiratokban – jellegével összhangban – a honvédelemmel, azon belül elsősorban a hadtudománnyal, nemzetbiztonsággal, hírszerzéssel, felderítéssel, katonai biztonsággal és a biztonságpolitikával kapcsolatos tudományos igényű kérdéseket feldolgozó és elemző írásokat – tanulmányokat, cikkeket és más tudományos területektémáit, anyagait – jelentejük meg;
- az írásmű legyen logikus, áttekinthető, tartalmilag összefüggő és jól tagolt;
- a témával kapcsolatos saját koncepció megfogalmazása legyen érthető, a következtetések pedig megalapozottak, érvekkel, adatokkal alátámasztottak legyenek.

Formai követelmények(és a kapcsolódó információk)**:**

- a szerzői kéziratok terjedelme lehetőleg ne haladja meg az egy szerzői ívet (40 ezer karakter, illetve 20-21 gépelt oldal); a kéziratot elektronikus formában Times New Roman 12 pontos betűkkel, másfeles sortávolsággal írva, a képeket és ábrákat feldolgozható (.jpg vagy .tif) formátumban kérjük megküldeni;
- lehetőség van a kézirat interneten történő megküldésére is, a **szakmaiszemle.kontakt@gmail.com** e-mail címen. A kézirathoz kérjük mellékelni a szerző vagy szerzők nevét, rendfokozatát, beosztását vagy munkakörét, állandó lakcímét, telefonon és interneten történő elérhetőségét;
- a közlésre elfogadott írásokért – a szerzői nyilatkozattal létrejött megállapodás figyelembe vételével – szerzői honorárium fizethető;
- a kéziratokat a Szerkesztőbizottság minden esetben lektoráltatja. A kiadványban megjelentetni kívánt írásokat a Szolgálat kompetens, tudományos fokozattal rendelkező munkatársai vagy más szakértők lektorálják;
- a Szerkesztőbizottság – a lektori vélemények figyelembevételével – fenntartja a jogot, hogy a megjelenésre alkalmatlannak ítélt kéziratokat – indokolás nélkül – nem közli. Az ilyen írásokat nem küldi vissza és nem őrzi meg;

- a kiadványban bárki publikálhat, akinek az írását a Szerkesztőbizottság az etikai, tartalmi és formai követelmények alapján, kiadványban történő megjelentetésre, valamint az interneten történő közzétételre alkalmasnak tartja. A közlésre nem került kéziratot csak az adott naptári év végéig őrizzük meg, de a szerző kérésére azt visszaadjuk;
- a közleményhez „Absztraktot/Rezümét" kell mellékelni, maximum 10–12 sorban, magyar és angol nyelven;
- a közleményhez 3–5 kulcsszó megadása szükséges, magyar és angol nyelven;
- az írás angol nyelvű címét is kérjük megküldeni.

Tudományos közleményekkel szemben támasztott formai követelmények

A folyóirat kizárólag az MSZ ISO 960 szabvány alapján készített hivatkozásokkal ellátott tanulmányt, cikket jelentet meg.

A közleményhez szükséges megadni, mellékelni:

A SZERZŐ, SZERZŐK NEVE (rendfokozata)
AZ ÍRÁS CÍME (magyarul, angolul)
ABSZTRAKT/REZÜMÉ (magyarul, angolul)
KULCSSZAVAK (magyarul, angolul)
SZERZŐI NYILATKOZAT

Bibliográfiai hivatkozás

A társadalomtudományokban a megszokott számozott hivatkozást az idézések jegyzetben[1] módszerrel kérjük alkalmazni.

Abban az esetben, ha a szerző nem ezt a módszert alkalmazza, a kéziratot lektorálás nélkül visszaküldjük átdolgozásra!

Idézések jegyzetben

A szövegen belüli idézést követően felső indexként megadott sorszámok jegyzetekre utalnak, melyeket a szövegbeli megjelenésük sorrendjében kell közölni. Ezek a jegyzetek tartalmazhatják az idézéseket.

Első idézés

Ha az idézések jegyzetben vannak megadva, egy dokumentumra vonatkozó első idézésnek tartalmaznia kell az idézés és a bibliográfiai hivatkozások külön jegyzékében levő kapcsolódó tétel pontos megfeleltetéséhez szükséges adatokat. Az első idézésnek tartalmazni kell: legalább a szerző(k) nevét és a teljes címet úgy, ahogy azok a bibliográfiai hivatkozásokban meg vannak adva, továbbá az idézett rész oldalszámát, ha az szükséges.

[1] Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. pp. 19-20.

Példák:

TARJÁN G. Gábor: A terrorizmus, p. 4.

KECSKEMÉTI Klára: A mediterrán térség és az Európai Unió, Európai Tükör, 2010. május XV. évfolyam 5. szám p. 38.

J. Nagy László: Mit kell tudni Algériáról?, Kossuth Kiadó, Budapest, 1987. p. 46-47.

PRYCE, Paul: France's Long War: Operation Barkhane, http://natoconcil.ca/frances-long-war-operation-barkhane/ (Letöltés ideje: 2015.02.24.),

Global Trend 2020: Mappingthe Global Future, http://www. foia.cia.gov/2020/2020.pdf (Letöltés ideje: 2012.08.21.),

Bibliográfiai hivatkozások jegyzéke

A bibliográfiai hivatkozások jegyzékében a hivatkozásokat az első adatelem betűrendjében kérjük megadni.[2]

Példák:

ÁCS Tibor: A reformkor hadikultúrájáról, *Budapest, 2005, Zrínyi Kiadó. ISBN 963 9276 45 6*

BEREK Lajos: A hadtudományi kutatómunka alapjai, In: SZILÁGYI Tivadar (szerk.): Szemelvények, Budapest, 1994, Zrínyi Miklós Katonai Akadémia. pp. 31–50.

KOVÁCS Jenő: Az új magyar hadtudomány gyökerei, fejlődésének szemléleti problémái, In: Új Honvédségi Szemle, 1993. 47. évf. 6. sz. pp. 1–7. ISSN 1216-7436

Global Trend 2020: Mappingthe Global Future, http://www. foia.cia.gov/2020/2020.pdf (Letöltés ideje: 2012.08.21.),

Ábra, vázlat, térkép, diagram, egyéb melléklettel szembeni követelmények:

- az ábra, vázlat címe;
- az ábra, vázlat forrás (vagy: Szerkesztette: …);
- az ábra, vázlat sorszáma (pl. 1. ábra.);
- idegen nyelvű ábra, vázlat esetén lehetőség szerint magyar nyelvű jelmagyarázat.

Rövidítések, idegen kifejezésekkel kapcsolatos követelmények:

- az idegen kifejezéseket, rövidítéseket magyarul és eredeti idegen nyelven kell az írásműben az első alkalommal feloldani lábjegyzetben;

Példa:

- WFP – (World Food Program – ENSZ Világélelmezési Programja).

SZERKESZTŐBIZOTTSÁG

[2] Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. p. 18.