KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT

XX. évfolyam 2. szám 2022. június

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 1021 Budapest, Budakeszi út 99-101. 1502 Budapest, Pf. 117
Telefon:	Dr. Kenedli Tamás 30/738-7925 Simon László 30/999-5205
E-mail:	szakmaiszemle.kontakt@gmail.com
Weblap:	https://www.knbsz.gov.hu/hu/publikaciok.html

HU ISSN 1785-1181

TARTALOM

DR. VIDA CSABA

A SOCMINT SZEREPE AZ ELEMZŐ-ÉRTÉKELŐ MUNKÁBAN
AZ ÚJ HÍRSZERZÉSI ÁG ELEMZŐ-ÉRTÉKELŐ MEGKÖZELÍTÉSE

Az elmúlt évtizedben egy újabb – napjainkra már önállónak tekintett – adatszerzési ággal bővült a nemzetbiztonsági szolgálatok információszerző rendszere. Az új hírszerzési ág az online közösségi hálózatokból történő információszerzésre szakosodott, így közösségi médiából történő adatszerzésnek (SOCMINT[1]) nevezték el. A SOCMINT kialakulása és fejlődése még mindig tart, mert az párhuzamosan zajlik a közösségi hálózatok terjedésével. Ennek ellenére már meg lehet állapítani, hogy ennek a hírszerzési ágnak egyre növekvő szerepe van a nemzetbiztonsági tevékenység számos területén. Sok esetben hiánypótlónak lehet tekinteni, mert olyan információkat tud biztosítani, amit a többi hírszerzési ág nem, vagy sokkal nagyobb erőfeszítéssel. Az új hírszerzési ág azonban új eljárásokat és módszereket követel meg nem csak az adatszerzés, hanem az adatfeldolgozás és az elemzés-értékelés területén is. Annak ellenére, hogy elméleti és gyakorlati szinten a SOCMINT már több, mint tíz éve létezik, még mindig nem történt meg teljes mértékben az elméletének a kidolgozása, amely összefügghet azzal, hogy a fejlődése szoros kapcsolatban van a közösségi média/hálózatok[2] kialakulásával is. Hasonlóságot lehet felfedezni, mikor több mint 100 évvel ezelőtt a rádióelektronikai felderítés (SIGINT[3]) kialakult. A SIGINT esetében is az elektromágneses kommunikáció fejlődésével tudott egyre fontosabb szerepet betölteni.

A közösségi hálózatok, amelyek a web 2.0[4] elemeinek tekinthetők, már az 1990-es években megjelentek, de csak a 2000-es években jöttek létre a jelenleg is meghatározó közösségi hálózatok. A 2010-es évektől azonban már alapvető szerepet töltenek be az információs társadalmunkban, vagyis az emberek közösségének alakításában. A közösségi hálózatok és a közösségi média nem tekinthető egymás szinonimájának, de kapcsolatuk elválaszthatatlan. A közösségi média egy olyan információtovábbító eszköz, amely az üzeneteit (információit) a közösség interakcióin keresztül terjeszti, míg a közösségi hálózatok az emberek közötti strukturált viszonyrendszer, amely biztosítja a közösség egyedei közötti kapcsolatot.[5] Tehát a közösségi média használja a közösségi (szociális) hálózatokat az információk továbbítására. Ezért a közösségi hálózatok mindig is részesei voltak az emberi társadalmaknak, de korábban ezek a hálózatok közvetlen perszonális szereppel rendelkeztek. Ennek ellenére csak a XX. század közepén alkotta meg a közösségi

1 Social media intelligence
2 Social media/Social networks
3 Signal intelligence
4 A web 2.0 olyan internetes szolgáltatásokat jelent, amelyek elsősorban közösségekre alapulnak, vagyis közös tartalommegosztáson. Ide tartoznak a fórumok és a chatek, valamint az online közösségi hálózatok is.
5 SCHAUER, Peter: 5 Biggest Differences between Social Media and Social Networking; https://www.socialmediatoday.com/social-business/peteschauer/2015-06-28/5-biggest-differences-between-social-media-and-social, (Letöltés ideje: 2022. 03. 25.)

hálózat fogalmát John Arundel Barnes ausztrál/brit antropológus[6], majd a fogalom a szociológia területén vált általánossá. Az online térben kialakuló közösségi hálózatok felhasználásával alakult ki a közösségi média, ami az online alkalmazások olyan csoportja, amely a web 2.0 elméleti és technológiai alapjaira épül. Továbbá a média különböző formáit képviselik, amelyeket a felhasználók internetes alkalmazásokon keresztül érnek el, illetve, mint végfelhasználók hozzák létre és módosítják.[7]

Az első internetes közösségi hálózatnak az 1995-ben Randy Conrads által létrehozott Classmate Online Inc. cég által üzemeltetett www.classmates.com[8] alkalmazást tekintik[9], de a közösségi hálózatok áttörése csak a 2004–2005-től következett be. A közösségi hálózatokról szóló szakirodalomban azonban éles vita van arról, hogy a közösségi médiának részét képezik-e az e-mailek, mivel akkor a közösségi hálózatok történetét 1971-ig az e-mailküldési protokoll beindításáig kell visszavezetni.[10] Véleményem szerint az e-mail más funkciót lát el, mint a közösségi média, mivel az email a magánlevelezés elektronikus változatának kell tekinteni. Az e-mail alapvető célja két vagy több személy számára információ továbbítása, és nem a közösségi kommunikáció. Természetesen az e-mailt használhatják a közösségi hálózatokhoz hasonló célokra is, de a fő funkciója eltér attól.

Az online közösségi hálózatok/média megjelenésével a nemzetbiztonsági rendszer látókörébe kerültek az ott megjelenő információk, mivel azok tartalmaztak olyan elemeket is, amelyek alapvetően érintik a biztonság kérdéskörét. Erre számos példa volt, többek között a terrortámadások megszervezése és előkészítése során is használták a hálózatokat. A 2010-es évek előtt, az első időkben a többi hírszerző ág foglalkozott a közösségi médiában megjelenő információkkal, amelyeket a saját eljárásaikkal és módszereikkel értek el. Ennek megfelelően alapvetően a nyílt forrású adatszerzés (OSINT[11]) és a kiberhírszerzés (CYBINT[12]) tekintette felelősségi területének, de a rádióelektronikai felderítés (SIGINT) és az emberi erőforrással folytatott hírszerzés (HUMINT[13]) is látott benne lehetőségeket. Az OSINT a közösségi médiában különböző keresőmotorok segítségével elérhető nyílt információk megszerzésére tett törekvéseket, míg a CYBINT a közösségi médiában nyíltan nem elérhető, főleg a felhasználók közötti kommunikáció felfedésére helyezte a hangsúlyt. A közösségi médiából történő adatszerzés azonban más jellegű eljárásokat és módszereket követelt meg, így megkezdődött egy új hírszerzési ág gyakorlati és elméleti alapjainak kialakulása.

---

6 John Arundel Barnes 1954-ben „Class and Committes in a Norwegian Island Parish" című tanulmányában fogalmazta meg a közösségi hálózat fogalmát. A tanulmány a Human Relations 1954-ben vol. 7. számában jelent meg a 39-58. oldalon.

7 KAPLAN, Andreas – HAENLEIN, Michael: Users of the World, Unité! The Challanges and Opportunities of Social Media; Business Horizons 2010/1. p. 61.

8 Az internetes honlap 1995. november 17-én alakult meg, amelynek célja az egykori osztálytársak felkutatásának elősegítése. 2015-ben 70 millió tagja volt.

9 RAJINDRA, Patil – SAJITHRA, K: Social Media – History and Components; Journal of Business and Management, 2013/1. p. 69.

10 Az első emailt 1971-ben Ray Tomlinson küldte, aki az internet elődjének az ARPANET fejlesztésével foglalkozott. Az email célja két fél (számítógép) közötti információcsere megvalósítása. https://www.guinnessworldrecords.com/news/60at60/2015/8/1971-first-ever-email-392973, (Letöltés ideje: 2022. 03. 22.)

11 Open source intelligence

12 Cyber intelligence

13 Human intelligence

Gyakorlati területen először a nemzetbiztonsági szolgálatokon belül az elhárítók, valamint a rendvédelmi erők közül a bűnügyi hírszerzők szorgalmazták a közösségi hálózatok megfigyelését és az információszerzés fokozását, mivel a terroristák és a bűnszervezetek egyre aktívabban használták a közösségi hálózatokat a kommunikációjukhoz (a bűncselekmények előkészítéséhez), valamint a propagandájuk terjesztéséhez. Ezért a rendvédelmi erők minden lehetőséget megragadtak arra, hogy minél több érdemi információt kinyerjenek a közösségi hálózatokból, de mivel célpontjaik többségében a saját állampolgáraik voltak, ezért nagyon nagy hangsúlyt kellett helyezni a személyiségi adatok védelmének garantálására. A fenti okok felgyorsították az önálló hírszerzési ág kialakulását, de hiányoztak az elméleti alapok, amelyek kidolgozása csak a 2010-es években kezdődött meg.

Elméleti területen a nemzetközi szakirodalom a közösségi médiából történő hírszerzés alapművének Sir David Omand, Jamie Bartlett és Carl Miller „Bevezetés a közösségi médiából történő hírszerzés (SOCMINT)[14]" című tanulmányát tekinti[15], amely 2012-ben jelent meg az „Intelligence és National Security" kiadványban. A cikk fogalmazta meg először a SOCMINT rövidítést, valamint vizsgálta a közösségi médiából történő hírszerzés szükségességét és legitimitását. A szerzők zömmel brit tapasztalatokon keresztül mutatták be a SOCMINT lényegét, amely során elhárító (rendvédelmi) szemszögből vizsgálták azt. Ezentúl Omandék a SOCMINT-et szétválasztották nyílt és nem nyílt információszerzéssé.

A SOCMINT elméleti kialakulását az is elősegítette, hogy a 2010-es években egyre több tudományos szintű mű elemezte és rendszerezte a közösségi média szerepét, helyét és lehetőségeit a társadalomban. A nemzetközi szakirodalomban 2018–2019-et követően már rendszeresen publikáltak a SOCMINT-ról. Magyarországon is ebben az időszakban kezdődött el a SOCMINT elméleti alapjainak lerakása, de eddig csak két tanulmány született[16] a témakörben, amelyek sajnos nagyon kevés kérdésben adnak választ az új hírszerzési ág kialakulására. Az első tanulmány[17] Erdész Viktorhoz köthető, aki 2018-ban a SOCMINT és a nyílt adatforrású információszerzés (többek között OSINT) kapcsolatrendszerére helyezte a hangsúlyt, valamint felvillantotta a SOCMINT lehetőségeit. A második, Dobák Imre és Tóth Tamás 2021-ben megjelentett tanulmánya[18] „Régi módszerek a kibertérben? (CYBINT-HUMINT, OSINT, SOCMINT, Social Engineering)" címmel is inkább a különböző hírszerzési ágak közötti kapcsolatokkal foglalkozott, mint a SOCMINT elméleti alapjainak megteremtésére, mivel az eredeti célja nem az volt. A fogalmi rendszer vonatkozásában is Erdész Viktorra hivatkozott. Tehát jelenleg hiányoznak azok a tanulmányok, amelyek a SOCMINT rendszerelvű feldolgozását mutatja be.

---

[14] Introducing Social Media Intelligence, amelynek a kiadója a brit Taylor&Francis vállalat. Az évente hét alkalommal megjelenő kiadvány alapítója 1986-ban Christopher Andrew volt.

[15] OMAND, David – BARTLETT, Jamie – MILLER, Carl: Introducing Social Media Intelligence (SOCMINT); Intelligence and National Security, 2012/6. pp. 801-823. ISSN 1743-9019

[16] A Magyar Tudományos Művek Tára (www.mtmt.hu) adatbázisa alapján történő keresés alapján, (Letöltés ideje: 2022. 03. 22.)

[17] ERDÉSZ, Viktor: A SOCMINT helye, szerepe az összadatforrású hírszerzésben; Felderítő Szemle, 2018/4. pp. 27-40.

[18] DOBÁK, Imre – TÓTH, Tamás: Régi módszerek a kibertérben? (CYBINT-HUMINT, OSINT, SOCMINT, Social Engineering); Belügyi Szemle, 2021/2. pp. 195-212.

Így jelenleg is a SOCMINT elméleti alapjainak lerakásánál tartunk Magyarországon. Véleményem szerint az elméleti keretek tisztázása nélkül nem lehet eredményes a közösségi hálózatból történő információszerzés gyakorlata.

A SOCMINT területe – közösségi média és hálózatok

Minden egyes hírszerzési ág saját információszerzési területtel rendelkezik, ahol speciális eljárásokkal és módszerekkel gyűjti a döntéshozók számára szükséges információkat, így korábban az emberek tudását a HUMINT, míg az elektromágneses hullámok rögzítésével a továbbított információkat a SIGINT, míg az információs rendszerekben tárolt védett információkat a CYBINT szerezte meg. A SOCMINT – ennek analógiájára – a közösségi médiából/hálózatokból teszkísérletet az információk összegyűjtésére.

Az internetes közösségi hálózatok olyan kapcsolati struktúrák, amelyek egyének és szervezetek kapcsolati rendszeréből állnak, de a kapcsolattartás színtere többnyire, de nem kivételesen egy internetes alkalmazás. Az online hálózatokban nincs mindig szükség konkrét ismeretségre (pld. rokoni kapcsolatra, osztályközösséghez vagy munkaközösséghez való tartozásra), mert lehetőség van olyan virtuális kapcsolattartásra, amelyek mögött nincs konkrét valós személyes ismeretség. Az online közösségi hálózatban általában olyan csoportosulások vannak, amelyek tagjai közös érdeklődési kör mentén szerveződnek, és lehetőség van az internetes alkalmazáson keresztül történő interakciókra (többek között kommunikációkra).[19] A hálózatok lehetőséget biztosítanak a csoporton belüli kommunikációra, információk továbbítására és cseréjére, az egyének részéről megosztott információk megjelenítésére, illetve a felhasználók kapcsolati körének bővítésére. Az információk megosztása különböző formátumúak lehetnek. Az online közösségi hálózatok abban is különböznek a személyes kapcsolatoktól, hogy nem korlátozzák a kapcsolatok számát az emberi kapcsolatok korlátai, amely a Dunbar-szám[20] alapján 150 körül (100–250 között) alakulhat, mert az online környezetben ez az szám 500-ra emelkedhet. Ez összefüggésben van azzal, hogy a mai felgyorsult (esetenként elkényelmesedett) világban sokkal egyszerűbb a virtuális tér felhasználása az ismerősökkel történő kapcsolattartásra, mint a személyes kapcsolattartás, mivel arra sokkal nagyobb energiát és időt kell fordítani, így sok személyes kapcsolat is a virtuális térbe helyeződött át. Ezáltal egyre népszerűbbé vált az online világ a kapcsolatok fenntartására és bővítésére. Megállapíthatók, hogy a virtuális közösségi hálózatok sokkal lazábbak, így azokba történő behatolás is sokkal egyszerűbb.

A közösségi hálózatok/média napjainkra egyre nagyobb szerepet töltenek be a társadalmakban, így a biztonsági szektorokra is jelentős hatással vannak. A közösségi média – társadalomformáló – fontosságát az is alátámasztja, hogy 2022 januárjában 4,2 milliárd felhasználója volt a különböző közösségi alkalmazásoknak[21], ami a föld

---

[19] VARGA, Gábor: Közösségi hálózatok II.; NSZFI, Távközlési szaktevékenységek – tankönyv, Budapest, 2008. p. 34.

[20] DUNBAR, Robin: How many friends does one person need? Faber and Faber, London, 2010. p. 302. ISBN 978 0 571 25343 2

[21] Most popular social networks worldwide as of January 2022, (Forrás: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Letöltés ideje: 2022. 03. 22.)

lakosságának (7,94 milliárd embernek[22]) a 43%-a. A felhasználók jelentős része 14 internetes alkalmazáshoz csatlakozott, amelyek tagsága egyenként meghaladja az 500 millió tagot. A legnépszerűbbek közé tartozik a Facebook (2,91 milliárd felhasználóval), a Youtube (2,56 milliárd felhasználóval), a WhatsApp (kétmilliárd felhasználóval), majd az Instagram (1,478 milliárd felhasználóval) és végül a TikTok (egy milliárd felhasználóval).[23] Emellett még számos közösségi hálózat létezik (Snapchat, Telegram, Pinterest, Twitter, Reddit, LinkedIn stb.), amelyek különböző funkciójuk miatt nagyon népszerűek. Ezeken kívül számos saját kínai alkalmazás létezik, de azok általában csak kínai felhasználók számára elérhetők.[24] A különböző alkalmazások esetében kettősség tapasztalható, mert egyrészről egymástól jelentősen eltérő szolgáltatásokat biztosítanak a felhasználók számára, így a közösségi hálózatok jellege széles spektrumon megtalálható. Másrészről a közösségi hálózatok között is verseny van a felhasználókért, így a sikeresebb hálózatok tulajdonságait próbálják átvenni mások, így a hálózatok közötti hasonlóság is fokozódik.

A közösségi média tipizálására a nemzetközi szakirodalom több választ ad, amelyek közül kettőt emelnék ki. Andreas M. Kaplan és Michael Haenlein hat csoportra osztja a közösségi médiát[25], amikor azokat a felhasználók jelenléte és megnyilvánulásainak mértéke alapján vizsgálták. Ez alapján megkülönböztetnek blogokat (pld. blogok és fórumok), kollektív projekteket (pld. Wikipedia), közösségi hálózati oldalakat (pld. Facebook), tartalomközösségeket (pld. Youtube), virtuális társadalmi közösségeket (pld. Second Life) és virtuális játékvilágokat (pld. World of Warcraft). Rajindra Patil a közösségi média elemeit tíz csoportra osztotta, amely szerint megkülönböztet: közösségi hálózatokat, mikroblogokat, blogokat, RSS-hírcsatornák, widgetek, linkelés és posztolás, tartalom értékelése, könyvjelzők alkalmazása, audió podcastok és videó podcastok.[26] Tendenciaként megállapítható, hogy a közösségi hálózatok/média fejlődésével egyre többfajta változatot lehet beazonosítani. Tehát a közösségi hálózatokat nem csak egyéni vélemény továbbítására, hanem közösségi kommunikációra, vagyis többoldalú interakciókra is alkalmazzák.

A közösségi média csoportosítása is megerősíti azt a tényt, hogy sokféle közösségi kommunikációs lehetőség (alkalmazás) áll rendelkezésre a felhasználók számára. Ennek keretében a fő hangsúly a felhasználók saját véleményének és álláspontjának továbbítására, valamint egyfajta magamutogatásra helyeződik, amely sokszor a valós élet egyfajta kompenzálása. A közösségi hálózatok lehetőséget biztosítanak a felhasználók számára, hogy ne mindig a valódi személyüket felfedve alkossanak véleményt, hanem annak elrejtésével, így egyrészről sokkal nyitottabban, míg másrészről sokkal több dezinformációt termelve kommunikálnak. A felhasználók többségét azonban jelenleg még nem jellemzi a biztonságtudatosság, így sokszor olyan bizalmas információkat is megosztanak, amelyek fontosak lehetnek a biztonság szempontjából.

---

22 Forrás: https://www.worldometers.info/world-population/ (Letöltés ideje: 2022. 03. 22.)

23 2022. januári adatok alapján. Forrás: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Letöltés ideje: 2022. 03. 22.)

24 Kínai közösségi hálózatokhoz tartozik: Wiexin (1,2 milliárd felhasználóval), Douyin (600 millió felhasználóval), QQ (574 millió felhasználóval), Sina Weibo (573 millió felhasználóval) és Kauishou (573 millió felhasználóval).

25 KAPLAN – HAENLEIN i. m. pp. 62-64.

26 RAJINDRA – SAJITHRA i. m. pp. 69-74.

A SOCMINT-információk jellege

Napjainkban megbecsülhetetlen mennyiségű információ keletkezik a közösségi hálózatokban, hiszen *„világszerte egy átlagos napon az emberek csak a Facebookon 4,5 milliárdszor Like-olnak, több mint félmilliárd alkalommal tweetelnek és 55 millió új fényképet osztanak meg az Instagramon."*[27] A Facebookon naponta 4 petabájtnyi (4096 terrabájtnyi) adat keletkezik.[28] Emellett talán még nagyobb mennyiségű mozgóképes információ kerül fel a különböző alkalmazásokra, illetve más közösségi hálózatokban is mérhetetlen információt osztanak meg. Megállapítható, hogy a közösségi hálózatokban lévő adatok jelentős része duplikált vagy többszörösen jelen van, így a keletkező adatoknak csak egy része számít új adatnak.

A közösségi médiában különböző formátumú adatok jellennek meg, amelyek lehetnek:

- rövid (esetleg néhány) karakterből/jelzésből álló üzenet (pl.: lájkolás);
- rövidebb szöveges üzenetek (reagálások és hozzászólások);
- hosszabb szöveges üzenetek (vélemények és álláspontok megfogalmazás – blog, fórum, poszt);
- hanganyagok (audio üzenetek);
- képek (korábban készített és esetleg módosított fényképek);
- rögzített videók (korábban készített és esetleg módosított mozgóképes felvételek megosztása);
- online közvetítések (eseményekről történő eredeti tudósítás);
- a felhasználók metaadatai (tartózkodási hely, közösségi hálózatokban eltöltött idő stb.).

Tehát megállapítható, hogy majdnem mindenfajta formátummal lehet találkozni a közösségi médiában, de az elmúlt évtizedben egy tendencia figyelhető meg, hogy a hangsúly a multimédiás formátumok felé tolódik el (lásd a TikTok népszerűsége), míg a hosszú szöveges üzenetek háttérbe szorultak. Ez összefüggésben áll azzal, hogy a felhasználók egy-egy megjelenésre (közlésre) minél kevesebb időt szánnak, és inkább a több megjelenést helyezik előtérbe. Emellett egyre inkább nagyobb hangsúlyt kapnak az online közvetítések, amely során a világ minden részéről élő közvetítés alapján lehet nyomon követni az eseményeket, több esetben a háborúkat is.

A fenti különböző formátumú információk – nemzetbiztonsági szempontból – az alábbi jellegűek lehetnek:

- a felhasználók profilja (magukról a felhasználókról megjelentetett személyes adat);
- a felhasználók által önként saját magukról megosztott információk (többek között élményeikről, tevékenységükről);
- a felhasználók a tartózkodási helyükről közölnek információkat (tudósítanak, posztolnak);

---

[27] pwc – Social listening www.pwc.com%2Fhu%2Fhu%2Fkiadvanyok%2Fassets%2Fpdf%2Fsocial_listening_2017.pdf&clen=3513686&chunk=true (Letöltés ideje: 2022. 03. 22.)

[28] OSMAN, Maddy: Wild and Interesting Facebook Statistics and Facts, 2021-es adat; https://kinsta.com/blog/facebook-statistics/ (Letöltés ideje: 2022. 03. 22.)

- a felhasználók saját véleményüket osztják meg egy adott témakörben (kommentálnak, hozzászólnak, blogolnak);
- szervezetek (magáncégek, állami szektor) közölnek információkat a felhasználók számára (tájékoztatás, propaganda, reklám);
- a hagyományos médiában megjelenő információk továbbterjesztése és véleményezése (hírfolyam);
- a felhasználók közötti interakciók, beszélgetés és információtovábbítás (pld. chatelések);
- a közösségi média felhasználóinak metaadatai (tevékenységi idő, bejelentkezések száma, tevékenység jellege);
- a hálózatokban lévő felhasználók aktuális tartózkodási adatok (helyadat).

A közösségi médiában látható, hogy nagyon széles az információtovábbítás lehetősége, amelyet nem csak információk megjelenítésére (publikálására), hanem kommunikációra is alkalmaznak. Megállapítható, hogy a megjelenített információ jellege is széles spektrumon helyeződik el, így a megfelelő kiválasztása is komoly kihívást okozhat. A közösségi médiában megjelenő témakörök jellege is rendkívül tág, hiszen nincs olyan témakör, amely ne jelenne meg benne. A megfelelő témakörök kiválasztására azonban már jelentős erőfeszítések szükségesek, ezért szükséges speciális eljárásokat, keresési módokat kidolgozni, hogy megtalálják az értékes információkat. Ez már a SOCMINT feladata, ami esetenként sokkal nehezebb, mint más hírszerzési ágak esetében.

A közösségi médiában nemzetbiztonsági – adatszerző – szempontból többfajta információt lehet beazonosítani, amelyek többek között eltérnek a védettségi szintjükben, hozzáférhetőségükben, megjelenésükben, illetve mennyiségükben. Ezáltal megkülönböztethetünk:

- a közösségi média minden felhasználója, esetenként nem csak a felhasználók számára elérhető – nyílt információk;
- a közösségi hálózatokban zárt körben terjesztett információk, amelyek csak az adott kisközösség tagjai láthatnak – enyhén védett információk;
- a közösségi hálózatokban meghatározott személyeknek továbbított információk, amelyek kizárólag a megcímzett személy(ek) láthatnak – védett információ;
- a közösségi hálózatokban a felhasználókra és tevékenységükre vonatkozó információ – a nyílttól a védett információig;
- a közösségi hálózatokban megjelenő metaadatok – erősen védett információk (többségében a szolgáltatótól megszerzett információ);
- a fórumokból és a hozzászólásokból (kommentekből) származó műveleti adatok.

A különböző információk más-más jellegű információszerzést követelnek meg, amelyhez a SOCMINT-nak eltérő eljárásokat és módszereket kell alkalmazni. Az információk összegyűjtésénél azonban nagyon fontos, hogy az információk/adatokat úgy kell megszerezni, hogy az információ birtokosa ne szerezzen róla közvetlen tudomást. Ez alól kivételt képez a fórumokból és a hozzászólásokból származó műveleti adatszerzés, mert annak egyik eljárása lehet a provokáció vagy a hozzászólók témaköri terelgetése. Nagyon fontos, hogy az adatszerzés ezen módszerei ne váljanak információs műveletté, vagyis befolyásolássá.

A SOCMINT fogalmi rendszere

A közösségi médiából történő információszerzés (SOCMINT) fogalmi rendszere vonatkozásában még nincsenek egységes meghatározások, de abban mindenképpen konszenzus van, hogy a SOCMINT önálló hírszerzési ág, amely az online közösségi médiában és hálózatokban megjelenő adatok és információk speciális módszerek és eljárások alapján történő összegyűjtésére irányul.

A SOCMINT pontos meghatározására a Sir David Omand-féle 2012-es cikk sem vállalkozik, hanem inkább a keretek meghatározásával foglalkozik, főleg az alkalmazási feltételekkel és lehetőségekkel. A tanulmány azért volt fontos, mert a hírszerző ágak között új területként határozta meg a SOCMINT-et, amelyet korábban az OSINT és a SIGINT közötti területen helyezett el. A SOCMINT-et a közösségi médiában megjelenő információk technikai eszközökkel történő gyűjtéseként, feldolgozásaként és elemzéseként definiálta, amelyet speciális programok és alkalmazások felhasználásával végeznek.[29] Sokkal pontosabb fogalmi rendszert találhatunk Teodor Tropotei és Ioan Deac által jegyzett tanulmányban[30], amely szerint *„a SOCMINT a közösségi oldalakon lévő online adatok azonosításával, gyűjtésével, összeállításával, hitelesítésével, ellenőrzésével és elemzésével foglalkozik, amely során beavatkozó és nem beavatkozó módszereket alkalmaz.”*[31]

A SOCMINT fogalmi rendszerénél nagy hangsúlyt kap a megszerzett információk szenzitivitása, így védelme, mivel sok esetben személyes adatok érhetők el vele. Ez abban az esetben kiemelt fontosságú, ha saját állampolgárokra vonatkozó adatokról van szó, főleg nemzetbiztonsági elhárító vagy rendvédelmi tevékenység esetében. A SOCMINT lehetővé teszi egyes személyek szoros megfigyelését, amely szintén jogi kérdéseket vet fel.

A fogalmi rendszerek vizsgálata során is megállapítható, hogy a SOCMINT nemzetbiztonsági hírszerző területen történő alkalmazása nem kapott eddig megfelelő hangsúlyt. A SOCMINT adatszerző képességeinek és lehetőségeinek elemzése során nem csak elhárító, hanem hírszerző területen hatékonyan alkalmazható, mert általa elérhetők olyan hírszerzési információk, amelyek támogathatják az ország értékeinek védelmét és érdekeinek érvényesítését.

A SOCMINT helye, szerepe

A közösségi médiából történő információszerzés a többi hírszerzési ághoz hasonlóan adatszerző-tevékenység, amely biztosítja a döntéshozók tájékoztatásához szükséges információkat. Tehát a SOCMINT egy adatszerzési ág, amely a hírszerzési ciklus keretében – az elemző-értékelő szervezet információigénye alapján – összegyűjti a szükséges információkat, amelyek alapját képezhetik az elemző-értékelő munkának a döntéshozók kérdéseinek megválaszolásában. Mivel a SOCMINT a jellegénél fogva olyan információkat is képes biztosítani, amelyeket más hírszerzési ágak nem, vagy csak nagy erőfeszítéssel, így nélkülözhetetlenné vált a

---

[29] OMAND – BARTLETT – MILLER i. m. p. 802.

[30] TROPOTEI, Teodor – DEAC, Ioan: Social Media in Intelligence Analysis; STRATEGIC IMPACT, 2019/1-2. pp. 69-78.

[31] Uo. p. 70

jelenkori nemzetbiztonsági tevékenységben, vagyis mind az elhárító-, mind a hírszerzőtevékenység keretében.

Elhárítás

Az elhárítótevékenységben már a 2000-es évek elején felhasználták[32] a közösségi hálózatok lehetőségeit, amely során egyes biztonsági szempontból veszélyes személyek és azok tevékenységének megfigyelésére felhasználták. Az elhárító szolgálatok és rendvédelmi erők monitorozták a közösségi médiát, hogy az ott megjelenő információkból állapítsák meg a negatív biztonsági tényezőket, mint például egy adott körzetben megjelenő társadalmi elégedetlenséget vagy megmozdulások előkészítését.

Elhárító/rendvédelmi szempontból hasznosak:[33]

- a biztonsági események (terrortámadások, bűncselekmények) körzetében tartózkodó felhasználók által posztolt információk, mivel azok többek között világos képet biztosíthatnak az elkövetőkről, az esemény aktuális helyszínéről és az esemény következményeiről;
- a közösségi médiában megjelenő információk felkutatása és értelmezése alapján megállapíthatók az egyes biztonsági veszélytényezők kialakulásának folyamata, mint például a radikalizáláshoz vezető folyamat megállapítása;
- valós idejű riasztás, mert reálidőben információt adhatnak negatív biztonsági események bekövetkeztéről, valamint egyes esetekben az esemény bekövetkezése előtt is biztosíthat információkat;
- közösségekbe történő betekintés lehetősége, amely nem csak a közösségek tagjaira vonatkozhat, hanem azok tevékenységére, így monitorozható a biztonsági helyzet;
- bűnelkövetés vagy bűnelkövetésre történő felkészülés beazonosítása a bűnelkövetők közösségi médiajelenléte és kommunikációja alapján.

Nagyon hasznosak lehetnek az elhárítás számára egy vizsgált személyre vonatkozó adatok, amelyeket a SOCMINT biztosítani tud. Hiszen amennyiben az adott személy aktív felhasználója a közösségi médiának, akkor nyomon követhető a tevékenysége, valamint bűnössége esetén egyre több terhelő információ szerezhető meg róla. Emellett a SOCMINT által monitorozhatók a látókörbe került csoportok tevékenysége és azok tagjai, főleg akkor, amikor napjainkban a kommunikációra egyre kisebb mértékben alkalmazzák a hagyományos telefont.

Az elhárítás és a rendvédelem területén a SOCMINT által összegyűjtött információk többsége személyes adatokhoz tartozik, így azok védelméről a jogszabályok nagyon szigorúan rendelkeznek. A személyi adatok védelmét a különböző országokban eltérő módon szabályozzák, így a SOCMINT-adatokra is más-más előírások vonatkoznak. Tehát számos országban a SOCMINT által történő információszerzésnek is jól dokumentáltnak kell lenni, valamint az összegyűjtött

---

[32] OMAND – BARTLETT – MILLER i. m. p. 802., Sir Omand tanulmányában is belbiztonsági veszélytényezőkkel kapcsolatos példákkal vezeti be a SOCMINT bemutatását.

[33] Uo. pp. 804–805. „The Opportunity of SOCMINT" fejezet.

adatok csak azokra a személyekre vonatkozhatnak, amelyekre megfelelő engedélyekkel rendelkezik az adott szervezet. Az adatok tárolására is hasonló szigorú feltételek vonatkoznak.

Hírszerzés

A SOCMINT fellelhető nemzetközi szakirodalma csak érintőlegesen foglalkozik az adatszerző ág hírszerzésben történő felhasználásával, így annak rendszere nem kidolgozott. A hírszerzés elméletéből levezetve azonban a SOCMINT értékes információkat tud biztosítani ennek a szakágnak is. A SOCMINT által biztosított információk jellegét vizsgálva megállapítható, hogy a döntéshozók információigényeinek megválaszolásához felhasználhatók, valamint támogatják a hírszerzési tájékoztatók elkészítését. Így hírszerző szempontból hasznosak lehetnek:

- külföldi célszemélyekre vonatkozó adatok, többek között a külföldi állami és katonai vezetők esetében;
- külföldi (politikai, gazdasági és katonai) csoportok tevékenységére, álláspontjukra és véleményükre vonatkozó információk;
- olyan, külföldön keletkező vagy fennálló biztonsági veszélytényezőkre vonatkozó információk, amelyek hatással vannak az ország biztonságára, kiemelten a transznacionális kihívások esetében;
- külföldi eseményekre vonatkozó olyan információk, amelyek a hivatalos közleményeken vagy hagyományos médián túli híreket biztosítanak.

Hírszerzés vonatkozásában is figyelembe kell venni az adatok védelmét, nem azért, mert külföldi személyekről történik az adatszerzés, hanem főleg azért, mert azt kell védeni, hogy milyen információk állnak rendelkezésre az adott esemény vagy az adott személy esetében.

A SOCMINT esetében azonban nehezen választható szét a tevékenységi terület az elhárítás és a hírszerzés vonatkozásában, mivel az információszerzés nem külföldön folytatott, vagyis nem ellenséges területen, így csak az információ témaköre, a felhasználók hovatartozása és az adatok megjelenésének helyszíne különböztetheti meg, hogy melyik szakág használja fel az információkat.

A fentiek alapján megállapítható, hogy a SOCMINT, mint hírszerző ág közel azonos szerepet tölt be a nemzetbiztonsági tevékenységben, mint a többi hírszerző ág (HUMINT, SIGINT, OSINT stb.). Így a korszerű elhárító és hírszerző munka mára elképzelhetetlen a közösségi médiákból származó információk felhasználása nélkül, mivel a SOCMINT-ből érkező információk értékesek a döntéshozók tájékoztatásához, valamint a biztonsági problémák beazonosításához.

A SOCMINT jellemzői, módszere

A SOCMINT, mint hírszerzési ág fő jellemzőihez tartozik:[34]

- **heterogén és helyettesíthető**, mert az információk fajtái széles spektrumon vannak, amelynek köszönhetően az adott információ többféle módon is megszerezhető;
- **általános**, mert bármely témakörben biztosít információkat;
- **méretezhető**, mert a vizsgálat területe könnyen kiterjeszthető vagy korlátozható;
- **flexibilis**, mert a vizsgálat tárgya gyorsan változtatható, nincs szükség az adatszerzési lehetőség hosszú idejű átszervezésére;
- **láthatatlan**, mert a közösségi hálózatok felhasználói nincsenek tisztában az információszerzésről;
- a közösségi **felhasználók ellenlépései**, mert aggódnak a személyes adatok megszerzése miatt.

A közösségi hálózatokból/médiából történő információszerzés főbb jellemzői is alátámasztják azt a megállapítást, hogy SOCMINT-ban hatalmas lehetőségek vannak, mert majdnem minden témakörben képes biztosítani információkat. További – a fentieken túli – meghatározó, hogy hatalmas mennyiségű adat megszerezhető vele, amelynek megbízhatósága széles spektrumon van. Ebből kifolyólag szükség van a SOCMINT-információk megbízhatóságának ellenőrzésére. A túl sok információ gátolhatja a hatékony nemzetbiztonsági tevékenységet, ezért a SOCMINT esetében is szükség van megfelelő adatfeldolgozási tevékenységre, hogy értelmezhető információkat biztosítson a SOCMINT az elemző-értékelők számára.

Sir David Omand a SOCMINT felosztása során négy fajta információszerzési módot különböztetett meg[35]:

- a közösségi hálózatokból/médiából történő nyílt információszerzést;
- a közvetlen megfigyelést folytató információszerzést;
- a fedett emberi forrást felhasználó információszerzést;
- a behatoló titkos megfigyelést folytató információszerzést.

A fentieket azonban ki lehet egészíteni a felhasználók metaadatait összegyűjtő adatszerzéssel, valamint a manipuláló fedett információszerzéssel. A hat fajta információszerzési mód különböző eljárásokat és módszereket követel meg, amelyek egy része más hírszerzési ágakban is megtalálható, de vannak olyan eljárások, amelyek egyedülállók és csak a SOCMINT-re jellemzők.

A SOCMINT folyamata, mint minden hírszerzési ág alapvetően négy szakaszból áll, amelyhez tartozik az adatszerzési lehetőségek kialakítása, maga az adatszerzés, az adatfeldolgozás és előértékelés, valamint a továbbítás az elemző-értékelő szervezet számára. Omand[36] is hasonló módszerrel vizsgálja a folyamatot, de azzal az eltéréssel, hogy a SOCMINT szükségszerűségének keretében az adatokhoz történő hozzáférést elemzi, majd összevonja az adatfeldolgozást és az elemzést, illetve a terjesztést, vagyis a felhasználókhoz történő továbbítás megelőzi az ellenőrzést és a felhasználást. A hírszerzési ciklus figyelembevétele alapján az eredeti folyamatot vizsgálom, így az

[34] OMAND – BARTLETT – MILLER i. m. pp. 816–817.
[35] TROPOTEI – DEAC i. m. p. 72
[36] OMAND – BARTLETT – MILLER i. m. pp. 807–816.

adatok ellenőrzését és vizsgálatát a feldolgozási és ez előértékelési szakaszban elemzem. Továbbá fontos megállapítás, hogy a SOCMINT nem tér el jelentős mértékben más hírszerzési ágtól amennyiben a hírszerzési ciklusban betöltött szerepét vizsgáljuk, mivel a SOCMINT is hasonló folyamatot tartalmaz.

Az **adatszerzési lehetőségek** kialakításával kezdődik a SOCMINT-tevékenység, mivel a megfelelő források/hálózatok felfedése nélkül nem lehet sikeres a tevékenység. Anélkül a SOCMINT nem lenne képes megfelelő információkat biztosítani vagy olyan nagy mennyiségű felesleges információt továbbítana a hírszerzési cikluson belül, amely megakasztaná magát a ciklust is. A források felfedéséhez tartozik a keresési mechanizmusok kialakítása, valamint a fedett tevékenységekhez szükséges legendák és álprofilok létrehozása is. A lehetőségek kialakítása inkább a közösségi hálózatok egyfajta feltérképezésére irányul, amelynek során többek között a források ellenőrzésére is sor kerül, hasonlóan az OSINT-hoz. Amennyiben elmarad, vagy nincs lehetőség a SOCMINT-en belül az adatszerzési lehetőségek felkutatására, akkor az meghatározza az adatszerzés eredményét is.

Az **adatszerzés** a SOCMINT esetében több nehézségbe is ütközik, amely ugyan más hírszerzési ágakban is jelen van, de itt sokkal nagyobb mértékben. Egyik a túlságosan nagy adathalmaz, amelyben nem mindig megoldás a szűrés és a válogatás, mert sok esetben arra a sok kis információra van szükség, például a terrortámadás környezetében megjelenő közösségi hálózati információkra. A szűrés és a válogatás is bonyolult eljárásokat követel meg, mert nagyon fontos, hogy az értékes információk ne essenek ki. Tehát az adatszerzésnél is az a cél, hogy az célzott legyen, tehát csak a releváns információkat kell megszerezni, valamint a SOCMINT különböző adatszerzési lehetősége közül a megfelelőt kell kiválasztani. A hírszerzési ágon belül az eltérő adatszerzési lehetőségek sokszor eltérő eljárásokat követelnek meg, de a módszerek esetében előtérbe kerülnek a statisztikai és a mintavételi eljárások, illetve a célpontkutatás. A SOCMINT esetében is lehetőség van az automatizált adatgyűjtő technikák alkalmazására, de azokhoz mindenképpen átfogó adatfeldolgozó rendszerek szükségesek. *(Ezért nem hatékonyak az üzleti szférában /reklámiparban/ alkalmazott módszerek.)*. A SOCMINT esetében másik kulcsfontosságú tényező: az adatszerzést úgy kell végezni, hogy arról az adat birtokosa ne szerezzen tudomást, de még csak utalást sem. A közösségi hálózatok működése alapján egyes esetekben (főleg nyílt információk vonatkozásában) viszonylag könnyű, de az információ birtokosa által nem nyílttá tett információk esetében már sokkal nehezebb, sokszor fedett módszereket kell használni, mint például a legenda vagy az álidentitás. Emellett jelentős különbség van az elhárító és a hírszerző szakág számára folytatott adatszerzésben, mert a személyi adatok védelme saját ország állampolgárai esetében alapvető emberi jogi kérdés, amelynek nagyon szigorú szabályai vannak, amelyek a SOCMINT által megszerzett információkra is vonatkoznak. Így elhárító szakág esetében komolyabb problémákkal kell megküzdeni, míg hírszerzés esetében csak akkor, ha a célszemélyek között saját állampolgár is van. Tehát a SOCMINT-adatszerzésnek is meg kell felelnie a törvényi előírásoknak.

Az **adatfeldolgozás** és az **előértékelés** nélkülözhetetlen a SOCMINT esetében, mert egyébként a hírszerzési cikluson belül a túl nagy mennyiségű használhatatlan információ akadályozná meg a döntéshozók tájékoztatásának lehetőségét. Az adatfeldolgozás legfontosabb része az adatszerzés során összegyűjtött információk rendszerezése, a relevánsak leválogatása, a részinformációk összeállítása, illetve a

statisztikai eljárásokkal történő előértékelés. A SOCMINT esetében főleg azért van szükség az adatfeldolgozásra, mert a többségében jelentős mennyiségű részinformációkat képes összegyűjteni az adott témakörben, amelyek önmagukban értelmezhetetlenek, míg összességükben értékes adatokat biztosítanak. Sok esetben megfelelő tendenciákat is meg lehet határozni. Az adatfeldolgozás esetében nagy lehetőségek vannak a mesterséges intelligencia és a gépi tanulás alkalmazásában, főleg a részinformációkkal kapcsolatban.

Az elemző-értékelő szervezetek számára történő **továbbítás** a legfontosabb eleme a SOCMINT-nek, mivel csak azokból az információkból lehet a döntéshozókat tájékoztatni, ami az elemző-értékelők számára rendelkezésre áll. Emellett a továbbított SOCMINT-információknak olyannak kell lenni, amelyek értelmezhetők az elemző-értékelők számára, mert amennyiben nem, akkor nagy valószínűséggel nem kerülnek felhasználásra. A továbbításhoz tartozik továbbá az olyan SOCMINT-információk azonnali megküldése a felhasználók számára, amelyekről azonnal tudniuk kell, mint például egy terrortámadás előrejelzése vagy más veszélytényező felbukkanása. Tehát a SOCMINT rendelkezik olyan képességgel, amely információkat biztosíthat az országok előrejelző és riasztórendszeréhez. Ezt támasztja alá, hogy a közösségi médiában napjainkban egyre fontosabb szerepe van a közbiztonságnak, mivel az elkövetők és az események tanúi is jelen vannak a hálózatokban, így nagyon sok információ összegyűjthető belőle.

A SOCMINT kapcsolata más hírszerzési ágakkal

A SOCMINT, mint a legújabb hírszerzési ág szoros kapcsolatban van a többi hírszerzési ággal, mivel vannak közös adatszerzési eljárások és közös területek, de mindenképpen önálló ágnak kell tekinteni. Ennek ellenére egyes hírszerzési ágak részéről még mindig vitatott a SOCMINT felelősségi területe. Ezáltal szoros kapcsolata van az OSINT-tal, a CYBINT-tel, a HUMINT-tal, az IMINT-tel és a SIGINT-tel.

Az **OSINT** esetében nagyon szoros a kapcsolat, hiszen a SOCMINT sok szakértő szerint az OSINT-ből vált ki. A SOCMINT nyílt információinak jellege megegyezik az OSINT információk jellegével, hiszen az információ birtokosa tisztában van azzal, hogy bárki számára elérhető. Ide tartoznak többek között a nyilvános posztolások. A SOCMINT nyílt információk helye azonban eltérő az OSINT információkétól, mert azok például nem a hagyományos médiához köthetők, mivel a struktúrája és helyszíne is eltérő.

A **CYBINT** esetében a zárt hálózatokba történő behatolás technikája esetében vannak azonosságok a SOCMINT-tel, mivel a SOCMINT egyik területe a zárt közösségi hálózatokból történő információszerzés, főleg a hálózaton belül egymásnak küldött üzenetek vonatkozásában. Emellett a jelszóval védett részekbe (esetenként profilokba) történő behatolás esetén is CYBINT-eljárások alkalmazhatók.

A **HUMINT** esetében az álprofilok kialakításához szükséges legendák megteremtésében vannak hasonlóságok, hogy a profilok hosszú távon fennmaradjonak dekonspiráció nélkül. Emellett a közösségi fórumokból történő információszerzés esetén is a HUMINT eszközrendszerét is fel lehet használni.

Megállapítható, hogy a HUMINT-eljárások alkalmazása jelentős hasznot eredményezhet a közösségi hálózatokban.

A **SIGINT** esetében főleg a nemzetközi szakirodalom egy része lát közös kapcsolódási pontot, mivel a közösségi hálózatok is elektromágneses hullámokon terjednek, főleg a mobiltelefonok kommunikációjának igénybevételével. Ennek a kommunikációnak a megfigyelése, valamint a telefonok helyszínadatainak meghatározása is a SOCMINT részét képezi. Véleményem szerint azonban a SIGINT és a SOCMINT között is megtalálhatók az elválasztó vonalak, mivel a mobiltelefonos kommunikációban a hagyományos telefonálás a SIGINT, az adattovábbítás a CYBINT, míg a közösségi hálózatokból származó adatok a SOCMINT területe.

Az **IMINT** esetében található a legkevesebb találkozási pont, de a közösségi médiában megjelenő képek vonatkozásában vannak olyanok, amelyekhez IMINT képfeldolgozó-képesség kell. Megállapítható, hogy a közösségi hálózatokban a felhasználók által készített és posztolt vagy továbbküldött képek nagyon hasznos információkat biztosíthatnak az adott esemény környezetéről, például egy erőszakos támadás helyszínéről.

Tehát megállapítható, hogy a hírszerzési ágak között szoros kapcsolat van, ezért fontos a felelősségi területek pontos elhatárolása, mivel hatékonyság szempontjából nem jó, ha párhuzamosságok vannak, vagyis ugyanattól a forrástól több hírszerzési ág is megszerezheti az adott információt.

SOCMINT és az elemző-értékelő munka kapcsolata[37]

Az elemző-értékelő szempontból a SOCMINT nagyon értékes információkat képes biztosítani a döntéshozók tájékoztatásához, de ahhoz az elemző-értékelőknek megfelelő információkkal kell rendelkezniük a SOCMINT képességéről. A többi hírszerzési ághoz hasonlóan a SOCMINT-nak is vannak előnyei és hátrányai a többi hírszerzési ághoz képest, amelyet a SOCMINT számára meghatározott információigények meghatározásánál az elemző-értékelőknek figyelembe kell venni, mert csak akkor lehet hatékony a közösségi hálózatokból történő adatszerzés. Az elemző-értékelők számára is fontos, hogy azoktól az adatszerzési ágaktól szerezzék be a szükséges információkat, amelyek rendelkeznek képességekkel azokhoz. Tehát a SOCMINT-nak azokat a jellemzőit kell megvizsgálni, amely meghatározza az adatszerzés képességét az összegyűjthető információk mennyiségét és minőségét.

A SOCMINT előnyének kell tekinteni:

- olyan információk is megszerezhetők, amely más hírszerzési ággal nem, vagy nagyon nehezen begyűjthetők;
- egy-egy eseményről a bekövetkezésének időszakában lehet – több szempontból származó – információt beszerezni;
- hatalmas mennyiségű információ megszerezhető vele viszonylag rövid időn belül;
- sok esetben költséghatékonyabb más hírszerzési ághoz képest.

---

[37] VIDA Csaba: A hírszerzési ágak elemző-értékelő megközelítése; Felderítő Szemle, 2016/3. pp. 77-93. A tanulmányban a többi hírszerzési ágak elemzése alapján végeztem el a SOCMINT elemzését.

A SOCMINT hátrányának kell tekinteni:

- a megszerzett információk ellenőrzésre szorulnak, mivel az információk megbízhatósága nagyon széles spektrumon van;
- sok dezinformációs – információs művelet – zajlik a közösségi hálózatokban, amelyek célja a befolyásolás;
- mindenképpen adatfeldolgozásra van szükség a megszerzett információk esetében, mert a részinformációk egyesével nem mindig értelmezhetők;
- sok esetben csak részinformációk összegyűjtésére van lehetőség, így szükséges más információszerzési ágak bevonása is;
- sokszor csak aktív – beavatkozó – műveletekkel szerezhetők meg a szükséges információk.

A fentiek alapján a SOCMINT tekinthető ez egyik legfontosabb információszerzési ágnak, amelyekkel nem csak kiegészítő, hanem elsődleges információkat kaphatnak az elemző-értékelők.

Összefoglalás

A közösségi hálózatból történő információszerzés elemzéséből meghatározható, hogy jelenleg a nemzetbiztonsági szolgálatok műveleti tevékenysége szempontjából már nélkülözhetetlen információszerzési lehetőség. A közösségi médiában olyan mennyiségű és minőségű információ megjelenik, amelyek jelentős mértékben támogathatják a döntéshozók tájékoztatását, sok esetben elsődleges információt biztosítanak egy veszélytényezőről vagy egy fontos eseményről, míg általában kiegészítő információt biztosít az elemző-értékelők számára, amellyel növelni tudják a tájékoztatóik színvonalát.

A SOCMINT teljes lehetősége még nem ismert, mivel a közösségi hálózatok is folyamatosan fejlődnek és átalakulnak, így változik az azokból származó információk jellege, mennyisége és minősége. Megállapítható, hogy az információk jellege egyre inkább a multimédiás tartalmakban (videófelvételekben) nyilvánul meg, amelyek fokozottabb mértékben követelik meg az adatfeldolgozást és az értelmezést. Már általánosságban alkalmazott deepfake-módszerek[38] beazonosításához mindenképpen átfogó ellenőrzésre és elemzésre van szükség. Emellett – a közösségi hálózatok térnyerésével – egyre több információt tud biztosítani az elemző-értékelők számára. Az információk mennyiségének növekedése a SOCMINT-ot egyre nagyobb kihívás elé állítja, hogy a megfelelő információt megtalálják a hatalmas információhalmazban. Ehhez mindenképpen szükségessé vált mesterséges intelligencia alkalmazása.

Az OSINT-hoz hasonlóan a SOCMINT jelentős rész nem csak a nemzetbiztonsági szolgálatok, hanem az üzleti szféra számára is információszerző területnek számít. Az üzleti élet a közösségi hálózatokat piackutatásra, a közvélemény igényeinek felmérésére is használják. Emellett a közösségi médiát egyre nagyobb mértékben felhasználja a politika, főleg választások idején, mert a politikai erők és szlogenek tesztelésére, illetve a politika és a társadalom közötti kommunikációra alkalmazzák. Napjainkra a közösségi hálózatok a felhasználóik számára elsődleges

[38] A képek és videóanyagok manipulálása.

információforrást jelentenek, mert egyre kevesebben követik a hagyományos médiát, miután a közösségi média válogatva (érdeklődési körüknek megfelelően) biztosítja a híreket.

A SOCMINT jelentőségéhez mérten Magyarországon még nem alakultak ki megfelelő elméleti alapok, és tudományos vita sincs a témakörben. A tanulmánynak alapvetően az volt a célja, hogy a közösségi médiából származó információszerzés területén egyfajta keretet biztosítson az elméleti vitáknak, amely során a nemzetközi és a hazai szakirodalmat és a nemzetbiztonság elméletét használtam fel. Továbbá a tanulmány célja a SOCMINT oktatásának megteremtése a Nemzeti Közszolgálati Egyetemen.

Felhasznált irodalom:

- DOBÁK, Imre – TÓTH, Tamás: Régi módszerek a kibertérben? (CYBINT-HUMINT, OSINT, SOCMINT, Social Engineering); Belügyi Szemle, 2021/2. pp. 195-212.
- DUNBAR, Robin: How many friends does one person need? Faber and Faber, London, 2010. p. 302. ISBN 978 0 571 25343 2
- ERDÉSZ, Viktor: A SOCMINT helye, szerepe az összadatforrású hírszerzésben; Felderítő Szemle, 2018/4. pp. 27-40.
- https://www.guinnessworldrecords.com/news/60at60/2015/8/1971-first-ever-email-392973 (Letöltés ideje: 2022. 03. 22.)
- https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Letöltés ideje: 2022. 03. 22.)
- https://www.worldometers.info/world-population/ (Letöltés ideje: 2022. 03. 22.)
- KAPLAN, Andreas – HAENLEIN, Michael: Users of the World, Unité! The Challanges and Opportunities of Social Media; Business Horizons 2010/1. p. 61.
- Most popular social networks worldwide as of January 2022. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Letöltés ideje: 2022. 03. 22.)
- OMAND, David – BARTLETT, Jamie – MILLER, Carl: Introducing Social Media Intelligence (SOCMINT); Intelligence and National Security, 2012/6. pp. 801-823. ISSN 1743-9019
- OSMAN, Maddy: Wild and Interesting Facebook Statistics and Facts, 2021-es adat; https://kinsta.com/blog/facebook-statistics/ (Letöltés ideje: 2022. 03. 22.)
- pwc – Social listening www.pwc.com%2Fhu%2Fhu%2Fkiadvanyok%2Fassets%2Fpdf%2Fsocial_listening_2017.pdf&clen=3513686&chunk=true (Letöltés ideje: 2022. 03. 22.)
- RAJINDRA, Patil – SAJITHRA, K: Social Media – History and Components; Journal of Business and Management, 2013/1. p. 69.

- SCHAUER, Peter: 5 Biggest Differences between Social Media and Social Networking; https://www.socialmediatoday.com/social-business/peteschauer/2015-06-28/5-biggest-differences-between-social-media-and-social, (Letöltés ideje: 2022. 03. 25.)
- TROPOTEI, Teodor – DEAC, Ioan: Social Media in Intelligence Analysis; STRATEGIC IMPACT, 2019/1-2. pp. 69-78.
- VARGA, Gábor: Közösségi hálózatok II.; NSZFI, Távközlési szaktevékenységek – tankönyv, Budapest, 2008. p. 34.
- VIDA Csaba: A hírszerzési ágak elemző-értékelő megközelítése; Felderítő Szemle, 2016/3. pp. 77-93. A tanulmányban a többi hírszerzési ágak elemzése alapján végeztem el a SOCMINT elemzését.

BABOS SÁNDOR

A NEMZETBIZTONSÁGI TEVÉKENYSÉG TÁRSADALOMTUDOMÁNYI MEGKÖZELÍTÉSE

A nemzetbiztonsági tevékenységet – azon belül a titkosszolgálati, úgymint a hírszerző és elhárító munkát – napjainkban többségében jogi-tartalmi szempontból, a részükre adott felhatalmazás, az alkalmazható eszköz- és módszerrendszer oldaláról, vagy történeti, azaz esettanulmányokon keresztül vizsgálják[1]. Mindazonáltal maguk a szolgálatok az állam, a titkosszolgálatok munkatársai pedig a társadalom szerves részét képezik. Mindezek miatt vonatkozásukban a szokásos jogtudományi, vagy némely esetben történettudományi megközelítés mellett érdemes politikatudományi, szociológiai, pszichológiai, filozófiai és pedagógiai, de akár közgazdaságtudományi szempontú kutatásokat is végezni. A társadalomtudományok felsorolás szerinti többségében már készültek olyan művek, amelyek kiindulási alapot jelenthetnek ehhez, azonban átfogó vizsgálatuk még várat magára.

A tanulmány célja a nemzetbiztonsági tevékenységet érintő legfontosabb társadalomtudományi kérdések és kutatások bemutatása, emellett javaslatok megfogalmazása a további kutatási irányokra vonatkozóan. Mindezek előtt azonban tisztázásra szorul a 'nemzetbiztonsági tevékenység' fogalma, mivel azt szélesebb körben a titkosszolgálati eszközök alkalmazásával azonosítják, mialatt tartalmát tekintve attól jóval bővebb kategória.

A nemzetbiztonsági tevékenység értelmezése

A nemzetbiztonsági tevékenység összességében felfogható a nemzetbiztonsági érdek érvényesítésére[2] kijelölt, és az abban egyéb érintettség, esetlegesen sajátos érdekviszony miatt részt vevő szervezetek és személyek ezirányú működéseként. Ahogyan a nemzetbiztonsági érdek magyar szabályozás szerinti fogalmából is levezethető, abban nem kizárólag a nemzetbiztonsági szolgálatoknak van szerepük, hiszen a függetlenség és a törvényes rend biztosításában többek között a Magyar

[1] DR. RÉVÉSZ Béla: Kutatások a sötétben. A titkosszolgálatok vizsgálatának módszertani kérdéseiről; Szegedi Tudományegyetem, Állam- és Jogtudományi Kar, Politológiai Tanszék, 2015. november 30-ai előadásának *2. kérdése: Mivel magyarázható az, hogy a politikatudomány nem tartja fontosnak a titkosszolgálati tevékenységek elemzését, az eddigi kutatások zöme pedig történeti vagy normativista irányból közelít a problémakörhöz?* https://u-szeged.hu/szabadegyetem/xvi-szemeszter/kutatasok-sotetben/kutatasok-sotetben?objectParentFolderId=28062 (Letöltés ideje: 2022. 05. 30.)

[2] Például Magyarországon a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény *74. § a) nemzetbiztonsági érdek: Magyarország függetlenségének biztosítása és törvényes rendjének védelme*

Honvédség[3], a törvényes rend védelmében a Rendőrség[4] is szerepet játszik. Megjegyzendő ugyanakkor, hogy napjainkban a biztonság, és így a nemzetbiztonság védelme sem teljesíthető kizárólag a fegyveres, rendvédelmi és titkosszolgálati szervek alkalmazásával[5], mivel azok olyan dimenziói is előtérbe kerültek, amelyek illetékesség okán más állami szervek (pld. médiahatóságok, a kibervédelmet az adott intézményben ellátó szervezeti egységek), több esetben a tevékenység egy részének kiszervezése révén polgári vállalkozások (pld. kritikus infrastruktúra fenntartási feladataiban közreműködők), továbbá mint a biztonságtudatosság egyik megnyilvánulási formája az egyén felelősségi körébe tartoznak[6].

Mindezeken belül kiemelten érdemes foglalkozni a titkosszolgálatok kormányzati irányításában részt vevő személyekkel – úgymint az irányító miniszterekkel, államtitkárokkal, a kormányzati egyéb szakmai vezetőkkel és tanácsadókkal. Esetükben a későbbiekben körülírásra kerülő biztonsági és pszichológiai, továbbá szociológiai nézőpontokat ugyan figyelembe vehetjük, azonban kiválasztásuk szempontjai nem egyeznek meg a titkosszolgálati dolgozókéval. Igaz azonban az is, hogy befolyástól mentes munkavégzésük nem biztosítható másképpen, mint a megfelelő felkészítéssel, és a jogszabályokban előírt biztonsági ellenőrzések lefolytatásával.

A nemzetbiztonsági tevékenység tehát olyan komplex, állami és nem állami szereplők részvételével folytatott, a nemzetbiztonsági érdek érvényesítésére irányuló folyamat, amely bár magában foglalja, de túl is mutat a titkosszolgálati eszközalkalmazáson, annak eredményeit döntéstámogató funkciójának betöltésében használja fel. E funkció értelmezhető a hírszerzés oldaláról a kormányzati döntésekhez szükséges információk biztosításaként és az elhárítás részéről a hatáskörbe utalt cselekmények, továbbá az azokhoz vezető kockázatok felderítéseként.

---

[3] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény *80. § 16. honvédelmi érdek: Magyarország biztonságát, katonai védelmi képességét meghatározó módon befolyásoló körülmények összessége, ideértve különösen a törvényes rend védelméhez, a függetlenség elleni támadó szándékú törekvések, a szuverenitást és területi integritást sértő vagy veszélyeztető törekvések elhárításához, a szövetségesi kötelezettségek teljesítéséhez, a szövetségi és honi védelmi infrastruktúra működésének, fejlesztésének biztosításához fűződő érdekeket*

[4] Magyarország Alaptörvénye (2011. április 25.) *46. cikk (1) A rendőrség alapvető feladata a bűncselekmények megakadályozása, felderítése, a közbiztonság, a közrend és az államhatár rendjének védelme.*

[5] „*...nemzetbiztonsági tevékenység nem rendőri tevékenység, nem titkosszolgálati tevékenység, hanem titkosszolgálati módszereket is alkalmazó döntés-előkészítő, döntéstámogató tevékenység, amiből következik, hogy a nemzetbiztonsági tevékenység elsődleges ismérve tehát nem a titok, a titkolózás, hanem az ország, a nemzet szolgálata, és maga az elnevezés is ezt testesíti meg."* In.: DR. JÁVOR Endre ezredes: A nemzetbiztonsági szolgálatok társadalmi megítélése, támogatottsága – a média szerepe a társadalom véleményalkotásának formálásában; Felderítő Szemle, 2009/2. p. 63.

[6] Lásd még: HÓDOS László: A nemzetbiztonsági szolgálatok közelmúltbeli tevékenységét befolyásoló mérföldkövek, avagy az új típusú biztonsági kihívások jelentette veszélyek és az azokra adott kormányzati, illetve jogalkotói válaszok 2010 és 2020 között; Szakmai Szemle, 2021/1. pp. 134-149.

Ilyen értelemben a nemzetbiztonsági tevékenység a társadalom olyan funkciója, amelyben a biztonság érvényesítésében érintettek szervezeti keretek között, vagy egyénileg részt vesznek. Fontos megjegyezni, hogy a demokratikus államokban e részvétel döntően az önkéntességen alapul. Mindez Magyarországon a rendszerváltás után történt szervezeti reformok nyomán alakult ki, mindaddig az állambiztonsági szervek tevékenységére és az állampolgárok nemzetbiztonsági (korábban állambiztonsági) tevékenységbe történő bevonása részben a megfélemlítésen, a negatív következmények kilátásba helyezésén alapult. A demokratikus átalakulás hozadékaként az emberi és állampolgári jogok érvényesülése és az állam átláthatóvá váló működése további katalizáló erőt jelentett a nemzetbiztonsági tevékenységben történő részvételi hajlandóság növelésére. Immár annak ellenére, hogy a titkosszolgálatok tevékenységének nagy részét a misztikum lengte körül, a rendszer nyilvános jogszabályokon alapuló működése megismerhetővé vált az állampolgárok számára is, a titkosság már nem a tevékenységi irányokra, vagy a jogtalan cselekmények elfedésére irányult, hanem a konkrét műveleti tevékenységgel kapcsolatos információk védelmére.

Mindezen változások pozitív következményeként a titkosszolgálatokkal való önkéntes együttműködési hajlandóság – kiemelten a terrorizmus és a szervezett bűnözés elleni tevékenységben – növekedett[7], a szolgálatok egyértelműen meghatározott alapfeladataival az emberek azonosulni tudtak, így a nemzetbiztonsági tevékenység részeként megindulhatott az a már 'szolgáltatói tevékenységnek' nevezhető munka, amely a biztonság garantálására irányult.

A társadalmi megítélés kérdései

A titkosszolgálatok által nyújtott szolgáltatás a biztonság, amelynek értékét az iránta való kereslet határozza meg. Tipikusan a nagyobb horderejű események után (pld. terrortámadások, helyi és globális hatású konfliktusok, kémügyek, kibertámadások) megnő az ezirányú társadalmi igény, amely általában olyan kormányzati lépéseket generál, amelyek a nemzetbiztonsági struktúra átalakítására, illetve többletforrások biztosítására irányulnak.[8] A társadalom részéről meglévő ilyen szükséglet (kereslet) azt is jelenti, hogy a közmegítélés szerint a közösség működésére valós befolyással bírnak olyan események, amelyek kezelése – legtöbbször megelőzése – funkcionális szervezet létét, vagy cselekvését kívánja meg. Ez a társadalom által támasztott igény azonban – napjainkban már különösen – maga után vonja a visszacsatolás követelményét is, amelyről gyakran megfeledkezünk.

---

[7] A nyilvánosság számára megismerhető ilyen tevékenységek például az Alkotmányvédelmi Hivatal Awareness Programja, az Amerikai Egyesült Államok 2007. évi Nemzeti Információmegosztási és Védelmi Stratégiájának (National Strategy for Information Sharing and Safeguarding) részeként működtetett Országos Gyanús Tevékenység Bejelentésére Irányuló Kezdeményezés (Nationwide Suspicious Activity Reporting Initiative).

[8] A terrorizmus kapcsán lásd még: BARTKÓ Róbert – FARKAS Ádám: A terrorizmus elleni harc nemzetközi jogi trendjei. In: FARKAS Ádám – VÉGH Károly (Szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020. pp. 115-132.

A titkosszolgálatoknak biztosított többletforrás mellett természetes és jogos igény a közösség részéről, hogy reális képet kaphasson a befektetése megtérüléséről természetesen olyan keretek között, amely a műveleti biztonságot nem veszélyezteti. Bár közvéleménykutatási adatok nem állnak rendelkezésre, de az utóbbi évtizedek tapasztalatai alapján elmondható, hogy a részletekbe menő tájékoztatás helyett többségében elegendőnek bizonyul az olyan nyilatkozatok kiadása, amelyek bemutatják a fejlődés irányait (pld. világszínvonalú titkosszolgálati eszközök beszerzése, az ország védelmi képességeinek erősítését biztosító kibervédelmi szoftverek vásárlása), azonban kellően általánosak is a konkrét műveleti tevékenység védelme érdekében. Meg kell ugyanakkor jegyezni, hogy amennyiben valamilyen nagyobb horderejű botrány körvonalazódik abban az esetben viszont részletes tájékoztatási igény jelenik meg a társadalom részéről (pld. Snowden-botrány, 9/11 kapcsán a titkosszolgálatok által elkövetett hibák).

A fenti közmegegyezésként is felfogható kettősség mellett ugyanakkor annak ellenére, hogy a társadalom nem fejt ki célirányos tevékenységet a titkosszolgálatok belső információinak megszerzésére, maga a titok léte információhiányt okoz az emberekben. Mindez, ahogyan Révész Béla is megállapítja[9], társadalmi feszültséget és információs vákuumot hoz létre, amelyet az emberi elme igyekszik kitölteni.[10] Ekkor válik az addig rejtett titkosszolgálati tevékenység misztifikálttá, jelennek meg azon fikciók, amelyek megfelelő kontroll nélkül az összeesküvés elméletek kialakulásához vezethetnek, vagy szándékosság esetén befolyásolási, illetve dezinformációs tevékenységet eredményeznek.

A biztonság és a munkaerő

A nemzetbiztonsági tevékenység sajátos körülmények között, egyedi eszközrendszerrel végrehajtott feladatai megkövetelik a magasabb fokú biztonsági rendszabályok betartását. Amennyiben el is tekintünk attól, hogy folyamatában jellemzően minősített adatok keletkeznek, akkor is figyelembe kell vennünk az ezen információk megszerzésére irányuló ellenérdekelt titkosszolgálati tevékenységet – a hírszerzést. Minden, a nemzetbiztonsági tevékenységet érintő adat ugyanis e szolgálatok érdeklődésére számot tart, és egyben ezek a legértékesebbek is egy idegen állam számára. Mint ilyenek pedig különösen védendőek, megszerzésük megakadályozása pedig az elhárítás legfontosabb feladata.

A nemzetbiztonsági tevékenység teljes folyamatában kiemelt jelentősége van tehát az adatok védelmének – a hírszerzés oldaláról azok megszerzésének –, amely az abban résztvevők oldaláról nagyfokú biztonságtudatosságot követel meg. Első olvasatban a nemzetbiztonsági tevékenységben részes titkosszolgálati munkatársak ilyenek, azonban a kérdést érdemes inkább generálisan vizsgálni, hiszen a szolgálathoz való tartozás kultúrája csupán egy felnőtt korban kialakított tanult viselkedési forma – nem is említve a nemzetbiztonsági tevékenységben részt vevő

---

[9] RÉVÉSZ Béla: A titok, mint politika. A titkosszolgálatok politológiai kutatásának lehetőségei; Doktori Disszertáció, Szegedi Tudományegyetem, Állam- és Jogtudományi Doktori Iskola, Szeged, 2007. p. 6.

[10] A pszichológia viselkedéstudományi ága szerinti attribúciós kényszer, hiba, torzulás: hajlunk arra, hogy akkor is okságot, szabályszerűséget, szándékosságot észleljünk, amikor az valójában nem áll fenn.

más személyeket, akik általában nem kapnak biztonságtudatosítási felkészítést –, mialatt teljes személyiségünk egész addigi életünkben fejlődött.

Amellett, hogy az adatok védelme érdekében nyilvánvalóan szükséges a biztonságtudatosítás, mind az állami, mind a civil szférában el kell végezni a célközönség szociológiai vizsgálatát is, hiszen eltérő oktatási módszereket kell alkalmazni az iskolai végzettség, a betöltött beosztás, az előzetes tapasztalatok és munkahelyek függvényében, mindamellett, hogy figyelembe kell venni a generációs különbségeket is.

A munkaerőpiacon jelenleg és a belátható időn belül aktív Baby Boom, X, Y, Z, Alfa generáció jellemzőinek mellőzésével,[11] azok közül csupán vizsgálódásunk szempontjából a legfontosabbakat kiemelve elmondható, hogy annak ellenére, hogy nem lehetséges éles határvonal meghúzása az egyes nemzedékek között, azonban tendenciózus fejlődési folyamatuk lekövethető. Az egyes generációk egyedileg jellegzetes magatartási formákat követnek, specifikus attitűdökkel rendelkeznek. A jelenleg aktív, azonban még fiatal generációk – Y, Z – az előző nemzedékektől élesen elkülöníthető preferenciákkal rendelkeznek. Ez főként a projektszemléletben érhető tetten, azon belül is a munkatársakkal – és kifejezetten a tehetséges munkatársakkal – való közös, alkotó tevékenység előtérbe helyezésében. Biztonsági oldalról vizsgálva e nemzedékeknél folyamatos az új technológiák iránti érdeklődés és azok használatának növekedése, amely folyamatosan újabb biztonsági kockázatok kialakulásához vezet.

A munkaerő megszerzése és megtartása szempontjából nézve szükségszerű a kimagasló munkatársak felvétele annak érdekében, hogy beinduljon a tehetségspirál,[12] amely további kivételes képességű személyeket vonz a szervezethez. Külön vizsgálandó kérdés az általános biztonságtudatosság és a magánéletbe való beavatkozás megítélése a fiatalabb generációkban, hiszen ezek is nagy hatással vannak a szervezetbe való bekerülés és a tényleges munkavégzés esetén. Általános rendezőelvként elmondható, hogy az újabb nemzedékek egyre kevésbé tolerálják a napi életükbe – különösen a kapcsolattartásukba – való (akár passzív) beavatkozást: *„a nyilvános egyre nyilvánosabb, a privát egyre inkább privátta válik”*.[13] Ez a tendencia visszavezethető arra, hogy az egyes generációk milyen körülmények között nőttek fel, ugyanis míg a Baby Boom és X generációk megtapasztalták a II. világháború utáni helyreállítás és a hidegháború nehézségeit, amelyek során biztonságuk az államtól és az általa bevezetett (jogkorlátozó) intézkedésektől függött,

---

[11] Lásd bővebben: ZALAI Noémi: Új típusú kihívások: generációváltás a nemzetbiztonsági szolgálatoknál; Nemzetbiztonsági Szemle 2016/1. pp. 34-44. https://epa.oszk.hu/02500/02538/00013/pdf/EPA02538_nemzetbiztonsagi_szemle_2016_01_034-044.pdf (Letöltés ideje: 2022. 05. 16.)
BABOS Sándor: Titkos felderítés a generációk tükrében. Szakmai Szemle 2018/4., pp. 17-26. https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_4_szam.pdf (Letöltés ideje: 2022. 05. 16.)
MCCRINDLE, Marc – WOLFINGER, Emily: The ABC of XYZ. Understanding the Global Generations; UNSW Press, 2009.

[12] A szociológiai kutatások szerint megnő a munkavállalási hajlandóság azokon a helyeken ahol köztudottan egy-egy kimagaslóan tehetséges személlyel lehet együtt dolgozni.

[13] SIMMEL, Georg: A titok és a titkos társadalom; In.: Simmel, Georg: Válogatott társadalomelméleti tanulmányok; Gondolat Kiadó, Budapest, 1973. p. 321.

addig a későbbi nemzedékek már az előzőekhez képest biztonságosnak nevezhető körülmények között nőttek fel.

Külön vizsgálandó kérdés – amelyet egyelőre csak részben lehetséges megválaszolni – a generációs különbségekből adódó problémák feloldása. A nemzetbiztonsági tevékenység különböző szintjein gyakran áll elő olyan állapot, amelyben a korábbi generáció széleskörű és hosszú titkosszolgálati tapasztalattal rendelkező tagja műveleti tisztként, vagy akár egy szolgálat vezetőjeként dolgozik, mialatt egy fiatalabb nemzedék tagja éppen e szolgálat kormányzati irányításában vesz részt. Az idősebb generáció tagja a tapasztalatot és a szolgálatban eltöltött időt tartja mértékadónak, míg a fiatalabb a projektspecifikus tényleges szaktudást és az együttműködési készséget. Mindez feloldhatatlan véleménykülönbséget okoz, amely végső soron a nemzetbiztonsági érdek sérelméhez vezethet.

A véleménykülönbség és a generációs feszültségek figyelmen kívül hagyása mellett nyilvánvalóan működőképes marad a hierarchikus rendben működő tevékenység, azonban hatékonysága mindenképpen csökken. A felek egymáshoz való közelítése a megfelelő oktatási rendszer bevezetésével részben megoldható, azonban véleményem szerint a feszültségeket végső soron csak a közös, huzamosabb ideig végzett munka oldhatja fel.

Pszichológiai kérdések

A nemzetbiztonsági tevékenységen belül a titkosszolgálati szférában már hagyományosnak nevezhető, hogy a felvételre tervezett személyek a szigorú biztonsági ellenőrzés mellett pszichológiai vizsgálaton is átesnek. Míg az előző a személy addigi életvitelére vonatkozó információkat, addig utóbbi a pillanatnyi lelki állapotot hivatott feltérképezni. Kiemelendő a 'pillanatnyi' kifejezés, hiszen a jövőre vonatkozó előrejelzések ugyan tehetők, továbbá a múltra vonatkozóan az interjúk során szerezhető be adat, azonban tényleges és objektív információk kizárólag a vizsgálat időpillanatában fennálló lelkiállapotra vonatkozóan szerezhetők be. A biztonsági ellenőrzés és a pszichológiai vizsgálat között mindazonáltal vonható párhuzam, ugyanis végső soron mindkettő a szervezet és a (nemzetbiztonsági) tevékenység során keletkező – döntően minősített – adatok védelmére irányul azáltal, hogy mindegyik megpróbálja kiszűrni azon személyeket, akik olyan kockázattal rendelkeznek, amely az elvárt mértékű titoktartás valószínűségét csökkenti.

A nemzetbiztonsági tevékenység teljes spektrumában – de különösen a titkosszolgálatok esetében – a pszichológiai megbízhatóság, lelki stabilitás kulcsfontosságú tehát a minősített adatok védelme szempontjából. Mindez természetesen nem csak a felvételi eljárásra vonatkozik, hanem az állomány rendszeres felmérésére és gondozására is. Ebben az esetben is párhuzamosan szükséges végezni a biztonsági szempontú ellenőrzést és a pszichológiai gondoskodást, hiszen szoros összefüggés áll fent közöttük. A kettő terület együttműködését több tényező is nehezíti – elsősorban a különleges személyi adatok kezelése okán –, azonban ezek szintetizálása a szakterületek között jogi normák szintjén megoldott.

A nemzetbiztonsági stratégiai szinttől elvonatkoztatva érdemes kitérőt tenni a tényleges műveleti munka pszichológiai aspektusaira is. Mindamellett, hogy a titkosszolgálati tevékenység jelentős része technikai jellegű, a szakemberek között megegyezés mutatkozik abban, hogy a minőségi (esetleg minősített) és időszerű információkat elsősorban a humán forrásoktól lehetséges megszerezni. Mind a hírszerzés, mind az elhárítás vonatkozásában igaz ez, és éppen ebből kifolyólag jelenthető ki, hogy a nemzetbiztonsági tevékenység taktikai szintjén a kapcsolatokkal való együttműködés elsődlegessége miatt kiemelkedően fontos a pszichológiai ismeretek és gyakorlat megléte. A humán erőforrás megfelelő vezetése, a velük való foglalkozás, sőt egyáltalán a megközelítésük olyan technikákat igényelnek, amelyek más foglalkozási ágakkal össze sem hasonlíthatók. Mindezen képességeket nyilvánvalóan a szervezett oktatásokon és tréningeken keresztül kell kialakítani, azonban megjegyzendő, hogy a szakma igazi fortélyai a tapasztalattal, vagy a tapasztalt kollégák iránymutatásaival alakulnak ki.

Végszó

A nemzetbiztonsági tevékenység társadalomtudományi megközelítésének átfogó vizsgálata több tudományág több tudományterületét érintő komplex feladat. A jelen tanulmányban bemutatott kérdések csupán napjaink legégetőbb problémáit érintik, azonban ezek további kutatása is rendkívüli erőkifejtést kíván meg.

Közhelyes, de a szituációt pontosan leíró értelmezés szerint a titkosszolgálati és a nemzetbiztonsági tevékenységet csak belülről lehetséges vizsgálni, azonban egy ilyen kutatás eredményeit nem lehet publikálni. A nyíltan megjelenő publikációk sosem lehetnek teljeskörűek, hiszen nem tartalmazhatják mindazt az információt, amely a nemzetbiztonsági szférán belül keletkezik.

Mindezek ellenére, véleményem szerint kijelenthető az, hogy napjaink legfontosabb, a nemzetbiztonsági tevékenységet érintő kérdései a generációs problémák kezelése, a biztonsághoz való viszony megváltozása, a pszichológiai felkészítés és a nyilvánosság tájékoztatásának kérdésköre.

Mindezek átfogó vizsgálata a korábban megjelenített tudományágak művelőinek közreműködését igényelné, amelynek megkezdéséhez szükséges a meghívásos szakmai konferenciák rendszerének kidolgozása.

Felhasznált irodalom:

- A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény
- A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény
- BABOS Sándor: Titkos felderítés a generációk tükrében. Szakmai Szemle, 2018/4. https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_4_szam.pdf (Letöltés ideje: 2022. 05. 16.)
- BARTKÓ Róbert – FARKAS Ádám: A terrorizmus elleni harc nemzetközi jogi trendjei. In: FARKAS Ádám – VÉGH Károly (Szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020.
- HÓDOS László: A nemzetbiztonsági szolgálatok közelmúltbeli tevékenységét befolyásoló mérföldkövek, avagy az új típusú biztonsági kihívások jelentette veszélyek és az azokra adott kormányzati, illetve jogalkotói válaszok 2010 és 2020 között; Szakmai Szemle, 2021/1.
- DR. JÁVOR Endre ezredes: A nemzetbiztonsági szolgálatok társadalmi megítélése, támogatottsága – a média szerepe a társadalom véleményalkotásának formálásában; Felderítő Szemle, 2009/2.
- Magyarország Alaptörvénye (2011. április 25.)
- MCCRINDLE, Marc – WOLFINGER, Emily: The ABC of XYZ. Understanding the Global Generations; UNSW Press, 2009.
- RÉVÉSZ Béla: A titok, mint politika. A titkosszolgálatok politológiai kutatásának lehetőségei; Doktori Disszertáció, Szegedi Tudományegyetem, Állam- és Jogtudományi Doktori Iskola, Szeged, 2007.
- DR. RÉVÉSZ Béla: Kutatások a sötétben. A titkosszolgálatok vizsgálatának módszertani kérdéseiről; Szegedi Tudományegyetem, Állam- és Jogtudományi Kar, Politológiai Tanszék, 2015. november 30-ai előadása https://u-szeged.hu/szabadegyetem/xvi-szemeszter/kutatasok-sotetben/kutatasok-sotetben?objectParentFolderId=28062 (Letöltés ideje: 2022. 05. 30.)
- SIMMEL, Georg: A titok és a titkos társadalom; In.: Simmel, Georg: Válogatott társadalomelméleti tanulmányok; Gondolat Kiadó, Budapest, 1973.
- ZALAI Noémi: Új típusú kihívások: generációváltás a nemzetbiztonsági szolgálatoknál; Nemzetbiztonsági Szemle 2016/1. https://epa.oszk.hu/02500/02538/00013/pdf/EPA02538_nemzetbiztonsagi_szemle_2016_01_034-044.pdf (Letöltés ideje: 2022. 05. 16.)

SUHAJDA ATTILA – DR. RITECZ GYÖRGY

A TERRORIZMUS ÉS A MIGRÁCIÓ (MENEKÜLTEK) KÖZÖTTI KAPCSOLAT ELEMZÉSE

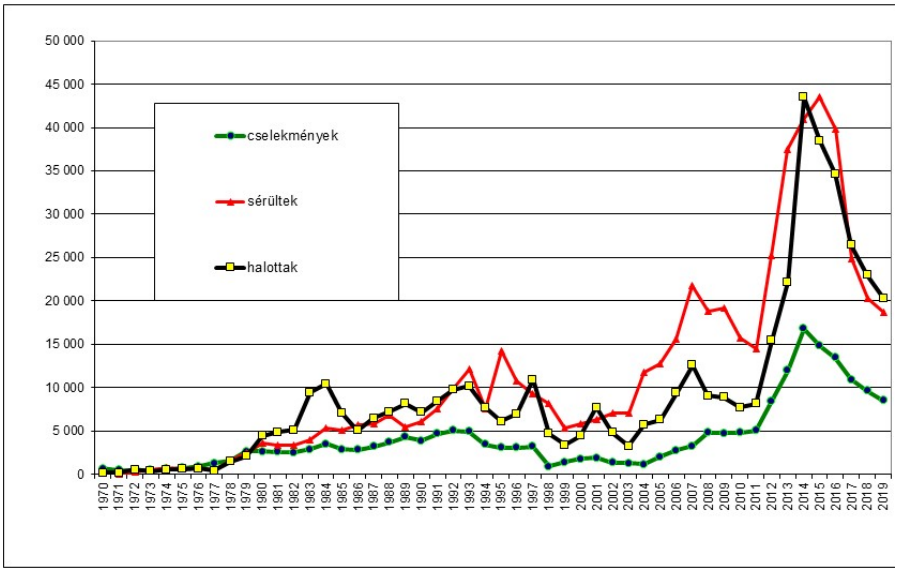
A tanulmány napjaink két fontos társadalmi jelenségének, a migrációnak és a terrorizmusnak kapcsolatát kívánja vizsgálni globális szinten, a kétpólusú világrend összeomlásától napjainkig, és kísérletet tesz az egyes trendfordulók meghatározására, és a mögöttes okok feltárására. A tanulmány bemutatja a migráció és a terrorizmus közötti ok-okozati viszonyt, legalábbis ami a hivatalos statisztikai adatok alapján feltárható, valamint ezek kapcsolodását a szélsőséges ideológiához. Az elemzés három mutató (terrorcselekmények száma, a menekültstátuszt kapott személyek száma, és a több adatból összevont menekülők száma) elemzésével próbálja megválaszolni a migráció és a terrorizmus közötti összefüggés jellegét.

Globálisan

Először talán célszerű megvizsgálni, hogy globális mértékben ténylegesen hogyan is alakultak a terrorcselekmények számai, és mit mutatnak a trendek. Ehhez meg kell jegyeznünk, hogy a terrorcselekmények vonatkozásában, főleg a nemzetközi összevetést lehetővé tevő, illetve a globális szintű és hitelesnek tekinthető adatok, adatbázisok száma igen szűkösnek nevezhető.[1] Jelen esetben alapvetően a tendenciát, illetve a nagyságrendet kívánjuk vizsgálni, ehhez a leghosszabb időintervallumot feldolgozó adatbázist, a Globális Terrorizmus Adatbázist (GTD)[2] célszerű felhasználni.

[1] A problémát jól érzékelteti: TÁLAS Péter: A terrorfenyegetettségről a számok tükrében. Nemzet és Biztonság, 2011/7. pp. 83-92.

[2] www.start.umd.edu/data-tools/global-terrorism-database-gtd (Letöltés ideje: 2010 és 2020. között évente) A letöltött adatok feldolgozása nyomán készített grafikonokat a szerzők szerkesztették, amelyekhez az Egyesült Nemzetek Szervezetének szakosított Menekültügyi Hivatala (United Nations High Commissioner for Refugees – UNHCR) – https://www.unhcr.org/hu/ menekültügyi adatai –, valamint a EUROPOL TE-SAT (European Union Terrorism situation and trend report) – www.europol.europa.eu – 2009-től 2021-ig megjelent kiadványai is felhasználásra kerültek.



1. ábra: A terrorcselekmények és áldozatok számának dinamikája 1970 és 2019 között

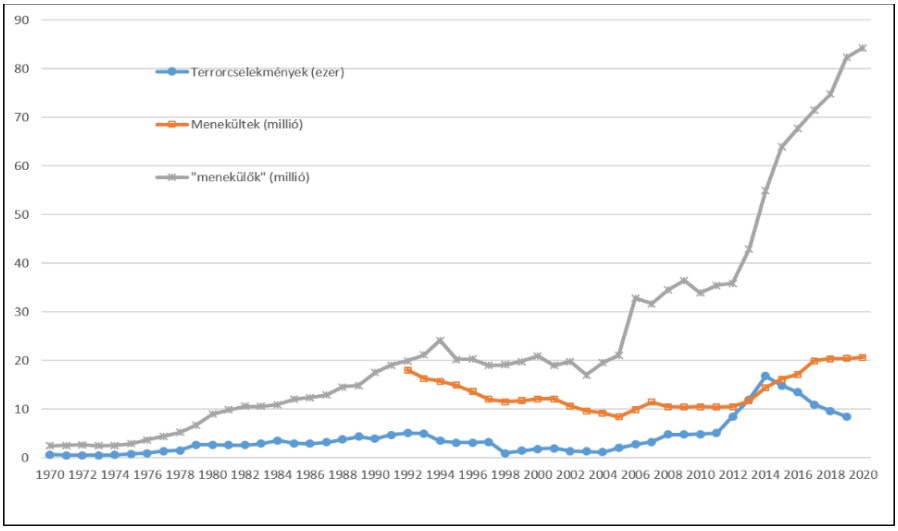
Az 1. ábra alapján szembetűnik, hogy a hidegháború időszakában évről évre egyre több terrorcselekmény történt a Földön (száma az évi néhány százas szintről az ötezres szintre nőtt), egészen a szocialista világrendszer összeomlásáig. Ezt követően tizenöt év enyhe csökkenés után (amelynek mélypontja 2004 volt 1159 terrorcselekménnyel) ismét, de már gyorsabban (négy év alatt, 2008-ra) megint megközelítette az ötezres szintet. Majd négy év stagnálás történt a cselekmények számában, miközben a terrorcselekmények kapcsán megsebesültek és meghaltak száma csökkent. 2011 után szinte „robbanásszerű" növekedést láthattunk, így 2013-ban 11.952, sőt 2014-ben már 16.818 terrorcselekményt regisztráltak világszerte. A halottak és sebesültek száma (külön-külön) meghaladta a negyvenezret. 2015-től viszont a globálisan elkövetett terrorcselekmények száma fokozatosan csökkent, ahogy a terrorcselekmények következtében meghaltak és megsebesültek száma is drasztikusan visszaszorult a korábbi évhez képest. Lényegében a 2014-15-ös csúcsértékek felére.[3] Az említett változások okait a migráció változásaival együtt igyekszünk elemezni.

A migrációs adatok elemzése előtt szükség van egy kis fogalomtisztázásra, ugyanis a médiában, politikában és a közvéleményben is több fogalom keveredik, illetve nem egyszer más a valós tartalma az éppen használt fogalomnak, mint amire a használó utal. Terjedelmi okokból részletes definíciókat nem ismertetünk (ezt megteszik helyettünk más tudományos igényű kiadványok[4]), inkább a különbségeket

[3] Talán meg kell említeni azt a tényt, mely nehezíti, de főleg a jövőben, nehezíteni fogja az ilyen fajta elemző munkát, hogy GDT elkészítésére 2019-től az USA kormánya nem ad támogatást, így azóta nem is frissül az adatbázis. A támogatás elmaradása talán úgy is értelmezhető, hogy a terrorizmusból eredő veszély, már nem jelent prioritást – a félévtizedes csökkenő trend miatt –, legalábbis egyes döntéshozók szerint.

[4] Például: RITECZ György – SALLAI János: A migráció trendjei, okai és kezelésének lehetősége 2.0.; Hanns Seidel Alapítvány, Budaörs, 2016.

igyekszünk érzékeltetni. Mindenki „migráns”, aki tartósan megváltoztatja a lakhelyét, akár belföldön, akár más országba teszi ezt. „Nemzetközi migráns”, aki más országba teszi át a lakhelyét, vagy mondhatnánk úgy is más országban él, mint ahol született. Lényegében ebbe a körbe tartozókat tekinti migránsoknak a köznyelv, ezt az is elősegíti, hogy az Egyesült Nemzetek Szervezetének szakosított Menekültügyi Hivatala (United Nations High Commissioner for Refugees – UNHCR) is ezt a definíciót használja. Pedig míg a szó eredeti és tudományos értelmében vett migránsnak nagyjából (csak becslések léteznek) minden tizedik ember tekinthető, addig a nemzetközi migránsok száma 2020-ban 280,6 millió volt.[5] Vagyis megközelítően minden harmincadik ember, tehát a migrációban részt vevők kétharmada nem is hagyja el az országát. És ezzel még nincs vége, ugyanis akik a migránsoktól féltik a biztonságot, nem is ezekre az embercsoportokra gondolnak, hanem egy jóval szűkebb rétegre, alapvetően az illegális[6] migránsokra, akiket sok esetben össze is kevernek a menedékkérőkkel, vagy a menekültekkel.[7] Ennek megfelelően inkább a tartalom és nem a forma alapján ez utóbbi kategória adatait vizsgáljuk, azzal együtt, hogy tudjuk, a menedéket kérők egy jó része legálisan lépi át az államhatárokat.



2. ábra: A menekültek, menekülők[8] és a terrorcselekmények számának, trendjének alakulása

[5] Az ismert adatok alapján (Nemzetközi Migrációs Szervezet – IOM: Világ migrációs jelentés 2000, 2010, 2020; Ritecz György: A Migráció a XXI. század kezdetén, Globe Edit, Saarbrücken, 2017.) az 1970-es 78,5 millióról lineárisan emelkedett a létszám, így a terrorcselekményekkel való bármiféle összefüggés lényegében kizárható.

[6] Pontosabban az irreguláris migránsokra, ugyanis tudományos megközelítésből a személy nem lehet illegális. Lásd: RITECZ – SALLAI i. m. pp. 11-22.

[7] Ez abból is adódik, hogy az illegálisan belépők zöme ténylegesen olyan országból indul, amelyben üldöztetésnek van kitéve, illetve a menekültügyi szabályokat (főleg az EU tagállamokban) felhasználva igyekeznek tartózkodási jogosultságot szerezni.

[8] A szerző által alkotott kifejezés, mely magába foglalja, a menekülteket, a menedék kérőket, a hontalanokat és az ún. belső kényszervándorokat. Lásd: RITECZ György: A Migráció a XXI. század kezdetén; Globe Edit, Saarbrücken, 2017. pp. 16-23.

Ahhoz, hogy megvizsgálhassuk, van-e összefüggés a menekültek számának alakulása[9] és a terrorcselekmények elkövetése (mennyiségi változása) között, először a hosszabb távú trendeket célszerű elemezni.[10] Az elmúlt félévszázad (2. ábra) első felében, lényegében a két világrendszer fennállásáig egyenletes, de enyhe emelkedés tapasztalható mind a menekültek, mind a terrorcselekmények vonatkozásában. 1992-től egyfajta trendforduló látható, amely után másfél évtizedig csökkenő trend érzékelhető mind a terrorcselekmények, mind a menekültek[11] számában. Mondhatnánk, (legalábbis ebből a szempontból) egyre békésebb világban éltünk, egyre kevesebb terrorcselekmény történt, és egyre kevesebb embernek kellett elmenekülnie az otthonából és a hazájából.

Ez így volt egészen 2003-2005-ig, ekkor viszont egy emelkedő tendencia indult el mindkét vizsgált kategóriában.[12] Ha az ábra nem is annyira érzékelteti, de az adatok egyértelműen ezt jelzik, ugyanis a terrorcselekmények száma a 2003-as 1262 cselekményről 2008-ra felugrott ennek közel négyszeresére (4788), miközben a menekültek száma még 2005-ig csökkent, de a következő két évben hirtelen 3 millióval megemelkedett, 11,4 millió főre. Eközben a menekülők száma hatványozottan nőtt meg (csak 2006-ban közel 12 millióval) és 2003-2008 között lényegében megduplázódott. A számok alapján is megállapítható, hogy másfél évtizede történhetett valami, hogy pontosan mi, erre később térünk ki. Az is kiolvasható az adatokból, hogy a menekültek és a menekülők száma egyfajta „fáziskéséssel" követi a terrorcselekmények növekedését.

Majd egy stagnálási fázis érzékelhető 2008-2011. között mind a két (illetve három) elemzett kategóriában. 2011-től a terrorcselekmények száma az addigi ötezer alatti értékről hirtelen nőni kezd, és 2014-re több, mint háromszorosára ugrik (16.818). A menekültek és a menekülők száma csak két évvel később, 2013-tól kezd emelkedni, főleg a menekülők száma, amely az utóbbi kilenc évben megduplázódott, és elérte a 84,3 milliót, miközben a menekültek száma lényegében 2017-re duplázódott meg, és tulajdonképpen azóta 20 milliós nagyságrendet képvisel. Vagyis 2014-2017. között is jelentős változást jeleznek az adatok, amely azt eredményezte, hogy innentől már a vizsgált kategóriák eltérnek egymástól. Ugyanis az utóbbi fél évtizedben a terrorcselekmények csökkenő tendenciát mutattak, amely nem is látszik megtörni, és már ismét 10 ezer alatti a cselekmények száma globálisan. A menekültek száma növekedés után stagnál, míg a menekülők száma töretlenül növekszik. E szerint meg tudtuk határozni azokat a csomópontokat, időszakokat, amelyek a fordulópontokat jelentették a vizsgált kategóriákban, illetve ahol „együtt futottak" és ahol már eltérnek. Ezek alapján azt mondhatnánk, hogy látszik összefüggés a terrorcselekmények és a menekültek számának változásai között.

A trendeket befolyásoló események, illetve a háttér vizsgálatát talán célszerűbb az utóbbi három évtizedre szűkíteni, annál is inkább, mivel azóta rendelkezünk

---

[9] Menekülthullámok korábban is voltak, például az 1946-1947-es évek fordulóján. A magyar–csehszlovák államhatáron kialakult menekültügyi válsághelyzetet mutatja be publikációjában Fórizs. Lásd: FÓRIZS Sándor: Menekültügyi válsághelyzet 1947-ben; Belügyi Szemle, 2015/2. pp. 149-163.

[10] Vizsgáltuk és az ábrán is feltüntettük a menekülteken (menekült státuszt megkapottak) kívül a „menekülőket" is mely kifejezés magában foglalja a menedék kérőket és az ún. belső kényszervándorokat (Internally Displaced People - IDP) is. Ez utóbbi teszi ki a menekülők zömét, 2020-ban 45,9 millió fő.

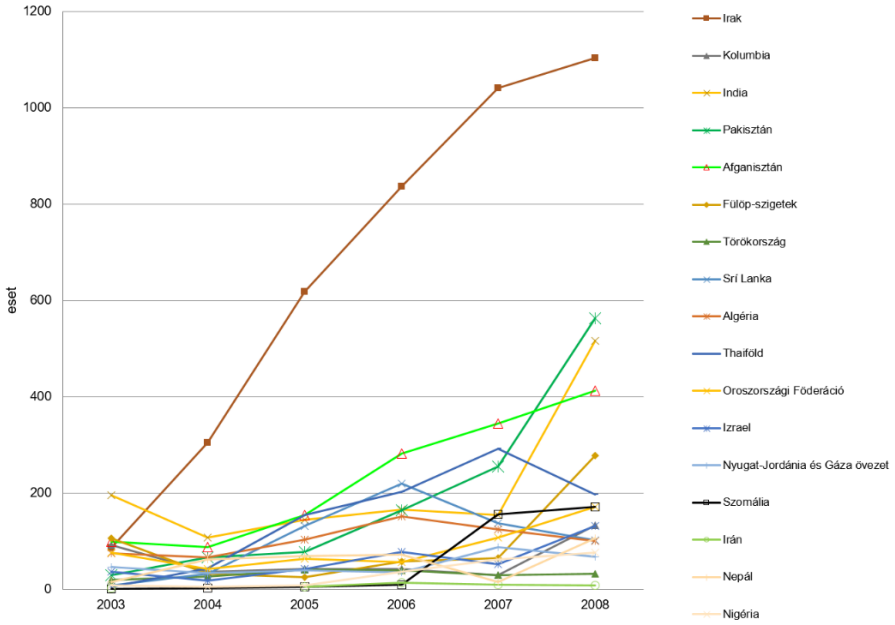
[11] Ekkortól szerepelnek egyes kategóriákra bontva a menekülők az UNHCR statisztikáiban. Addig (1951-től) csak a menekülteket tartották nyilván, illetve 1965-től a visszatérőket is.

[12] Az ismétlések elkerülése érdekében az okokról később ejtünk szót.

viszonylag kellő mennyiségű és hitelesnek is tekinthető információkkal.[13] A kétpólusú világrendszer megszűntét követő egyfajta normalizálódó időszakban[14] egyre kevesebb terrorcselekményt követtek el, és egyre kevesebb embernek kellett menekülnie. Ebből viszont egyértelmű ok-okozati összefüggést nem állapíthatunk meg.

A következő meghatározó és fordulópont az előző évtized közepe, amikortól (az adatok alapján) egyre veszélyesebb lett az élet bizonyos helyeken (erre még visszatérünk), és amikor látszott, hogy ez nem is lesz jobb, sokan elindultak egy biztonságosabb helyet keresni maguknak. Ez indokolja a „fáziskésést" is. A stagnáláson véleményünk szerint nincs mit magyarázni, egyértelmű. Ahogy az is, hogy a 2011 utáni terrorcselekmények drasztikus elszaporodásának logikus következménye lehetett a menekültek számának megemelkedése. De csak akkor feltételezhetjük az ok-okozati összefüggést, ha a terrorcselekmények helyszíne és a menekülők származási helye korrelál. Ehhez viszont célszerű ez egyes időszakokat külön-külön elemezni.

Az első növekedési hullám

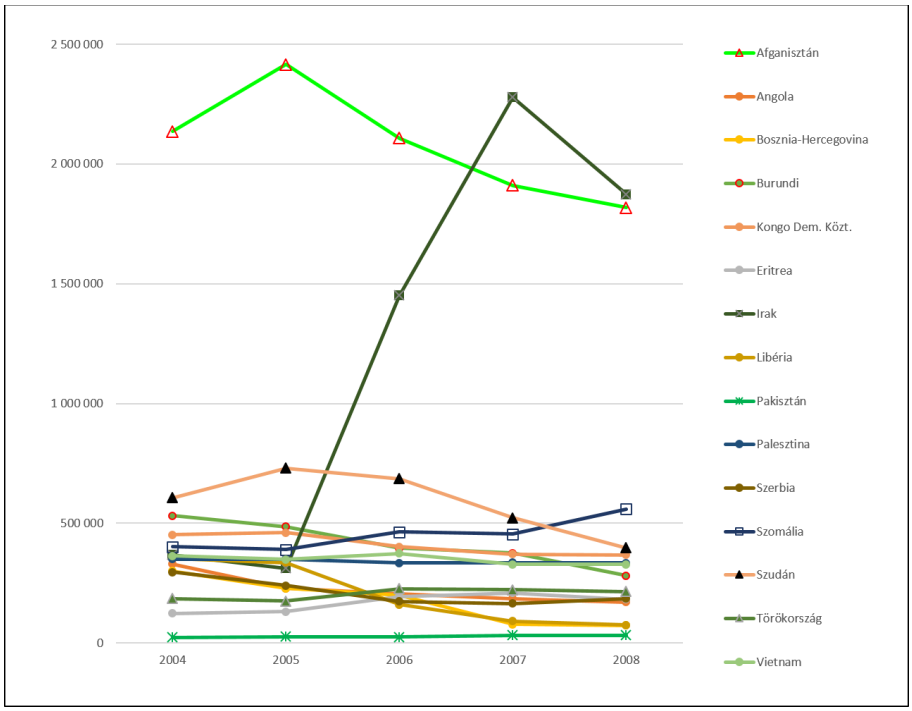


3. ábra: A terrorcselekmények alakulása a „legjellemzőbb" országokban 2003–2008 között

[13] BAKÓCZI Antal: Megismerési akadályok a terrorizmus kutatásában; Belügyi Szemle, 2015/7-8. pp. 88-105.

[14] A globális adatok lényegében nem érzékeltették az amúgy súlyos helyi konfliktusokat, pld. délszláv események, Ruandai népirtás.

Nehéz volt olyan grafikont szerkeszteni (3. ábra), amely hűen megmutatja a 2004–2008 közötti terrorcselekmények dinamikájának jellemzőit. Így végül 17 ország adatait tüntettük fel, mivel a vizsgált időszakban ezekben fordult elő az évi százas terrorcselekmény-nagyságrendet meghaladó adat, illetve esetükben érzékelhető az emelkedő trend. A 2003. évi adatot is felvettük, éppen azért, hogy látható legyen a 2004-es „mélypont" is. Ez utóbbi alapvetően India 2003. évi kiemelkedő adatából eredt, majd utána csökkenés, stagnálás jelentkezett itt, de 2008-ban a világon elkövetett terrorcselekmények rangsorában India már a harmadik helyen szerepelt. Ennek viszont el kell gondolkodtatnia bennünket arról, hogy itt, Európában mennyire is vagyunk tisztában a terrorcselekmények számával, helyszíneivel. De – ami a lényeg valójában – jól látható a grafikonon, hogy a 2004–2008 közötti időszakban jelentkező terrorcselekményszám-növekedés zömében az Irakban elkövetett cselekményekből eredt. Ez kitűnik abból is, hogy a világon nyilvántartott összes terrorcselekmény „csak" 6,9%-át követték el Irakban 2003-ban, majd 2005–2007 között már 30-32%-át itt követték el. Ezt egészítették ki a 2005-től növekvő mértékű afganisztáni, illetve a 2007–2008-tól emelkedő számú pakisztáni merényletek. (Valamint a már említett indiai emelkedő trend.)



4. ábra: A menekültek adatai a „legjellemzőbb" származási országok szerint 2004–2008 között

A menekültek adatainak illusztrálásához csak egy nehezen átlátható grafikont (4. ábra) tudtunk készíteni, de talán így érzékeltethető igazán a nagyságrendek és a változás dinamikája. Itt 15 országból áll a „legjellemzőbb" származási országok listája, vagyis amelyek a legtöbb menekültet bocsátották ki ebben az időszakban. Annyiban mindenesetre szemléletes a grafikon, hogy míg a világ összes

menekültjének adatai emelkedtek ezen időszakban, addig a legnagyobb kibocsátó országokból lényegében évről évre közel azonos nagyságrendű, vagy egyre kevesebb menekülőt tartottak nyilván. Kivéve Irakot, amely szinte más dimenzióban található, sőt az itteni emelkedés is lényegében 2006-2007-re koncentrálódott. Ez utóbbi azt is jelenti, hogy a korábbi éves 300 ezres menekültszámról 2007-re ennek hétszeresére, 2,28 millióra nőtt az innen elmenekültek száma. Ezzel a világon regisztrált menekültek arányán belül a korábbi 3,6%-ról hirtelen 23,5%-ra ugrottak, ami azt jelenti, hogy 2007-ben a földön minden negyedik menekült Irakból származott. A grafikonból az is jól érzékelhető, hogy Afganisztán tartósan egy más nagyságrendet képviselt, mint a többi „főbb" menekülteket kibocsátó ország, mivel tartósan 2-2,5 millió menekült szerepelt a regisztrációkban ezekben az években. Az adatok értékeléséhez meg kell jegyezni, itt nem az adott évben benyújtott új menedékkérelmekről van szó, hanem az adott év végén (december 31.) menekültként nyilvántartottak számáról.

A részadatokból jól érzékelhető, hogy teljes együttmozgás nem mutatható ki[15] a terrorcselekmények és a menekültek száma között, de a változások dinamikája igazán egy országhoz, vagyis Irakhoz köthető, mind a kettő területen. Rajta kívül még Afganisztán említendő meg, ahol láttuk, hogy a vizsgált időszakban közel ötszörösére nőtt a terrorcselekmények száma, és ennek is köszönhető, hogy menekülők millió i hagyták el az országot. Jól érzékelteti ennek a térségnek a kiemelkedő szerepét az is, hogy e két országban elkövetett terrorcselekmények számaránya (a világban elkövetett – GTD-ben regisztrált – összes cselekményhez képest) ekkor ugrott meg 14,7-ről 42,8%-ra. Vagyis 2007-ben a világban elkövetett minden terrorcselekmény közel felét az ezen két országban élőknek kellett elszenvednie. Ugyanezen időszakban, ugyancsak az e két országból menekülők aránya (az ENSZ által regisztrált menekültekhez képest) 26,2%-ról 43,3%-ra emelkedett. Ez azt mutatja, hogy mégiscsak a terrorcselekmények az egyik legnagyobb indukáló tényezői a menekülésnek ebben az időszakában. Ezzel együtt talán érdemes leírni, mi is történt ekkoriban ezekben az országokban.

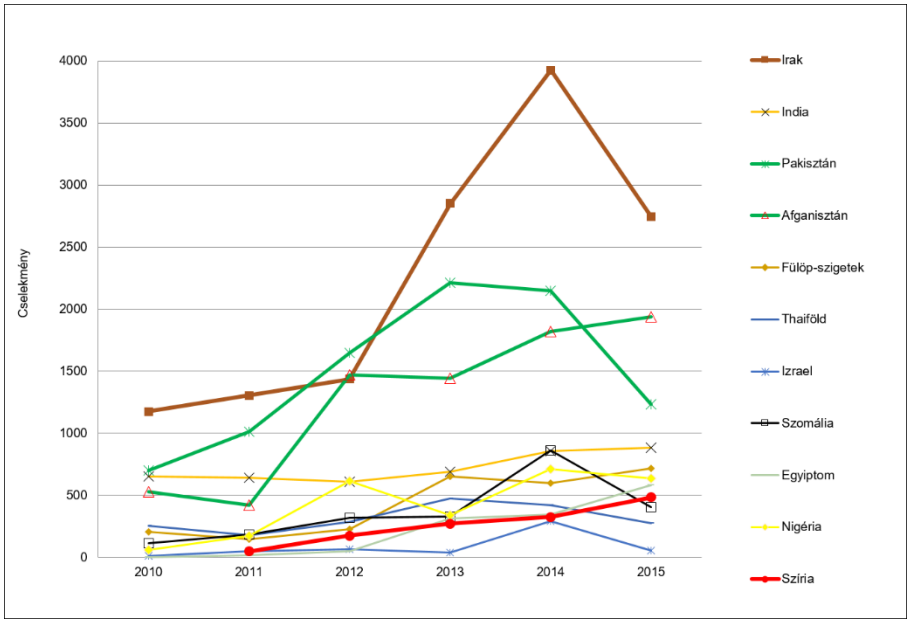
Köztudott, hogy a 2001. szeptember 11-i USA-beli terrortámadásokat követően az Egyesült Államok „háborút hirdetett" a terrorral szemben. Ennek szellemében szövetségeseivel lerohanta előbb Afganisztánt (2001), majd Irakot (2003). Az afganisztáni tálibok és az Al-Kaida erőinek jelentős része átmenekült a szomszédos Pakisztánba.[16] Pár évvel később, mikor a „megtámadott" erőknek sikerült kicsit rendezniük soraikat – és a megszálló, „felszabadító" erők aktivitása csökkent –, mondhatni, ellentámadást indítottak. Ez látható 2004-től a terrorcselekmények statisztikáiban, majd a menekültek adataiban is. 2009-től viszont új elnöke lett az USA-nak, aki kicsit más módszereket igyekezett keresni a terror elleni küzdelemre. Lényegében Obama elnök abbahagyta a háborút, és megkezdte a kivonulást Irakból, majd Afganisztánból is. Meglátásunk szerint ezt tükrözi a stagnáló időszak a terrorcselekmények és a menekültek statisztikáiban egyaránt. Aztán jött 2011, az ún. „Arab tavasz", de lássuk a statisztikákat!

---

[15] Akkor lehetne kijelenteni az egyértelmű összefüggést, ha minden országban, ahol nőtt a terrorfenyegetettség, növekedne a menekülők száma is, de ez nem így van. Jól jelzi ezt például India esete, ahol magas a terrorcselekmények száma, a nemzetközi statisztikákban regisztrált menekültek száma viszont elenyésző.

[16] Illetve más velük szimpatizáló országba, mely nem kis mértékben hozzájárul a 2011 utáni eseményekhez.

A második növekedési hullám

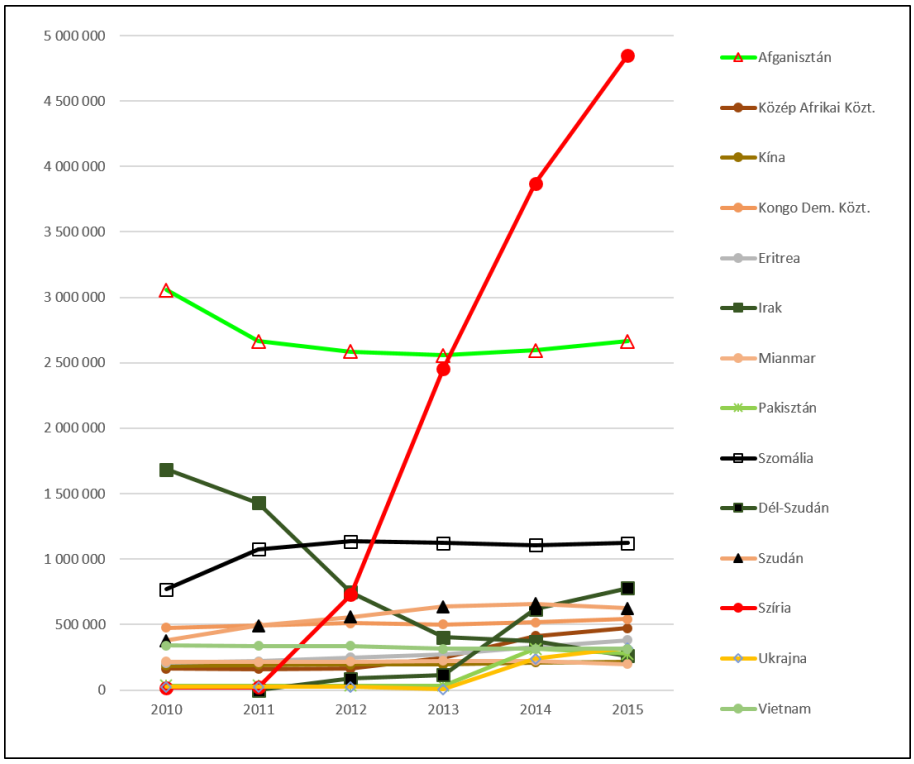


5. ábra: A terrorcselekmények alakulása a „legjellemzőbb" országokban 2010–2015 között

Maga az „Arab tavasz" eseménye a statisztikai adatok (5. ábra) szerint jelentős számú terrorcselekménnyel nem járt, sőt Észak-Afrika és a Közel-Kelet országai közül a TOP 10-be csak Egyiptom és Izrael került be. A 2012 utáni drasztikus megugrás valójában a már említett „hármasnak", Iraknak, Afganisztánnak és Pakisztánnak köszönhető. A világon regisztrált összes terrorcselekmény több mint fele (50–54,5%) ebben a három országban történt azokban az években. Igaz, ez idő alatt Szíriában is tízszeresére nőtt a terrorcselekmények száma (49-ről 485-re), de ez még mindig „csak" töredéke az irakiak által elszenvedett cselekményeknek. Bár azt is meg kell jegyezni, hogy a terrorcselekmények során meghaltak és megsérültek számát tekintve Szíria már a negyedik a 2012-2015-ös években. Mindez szoros összefüggésben van az Iszlám Állam (ISIS) és elődszervezeteinek tevékenységével. Érdekes megfigyelni, hogy a 2014-es adatokhoz képest Irakban és Pakisztánban is jelentősen (30, illetve 42,4%-kal) csökkent az elkövetett terrorcselekmények száma 2015-ben. Ez viszont annak is köszönhető, hogy az euroatlanti (korántsem egységes) politikai vezetők érzékelték, hogy az addig (leginkább nem nyílt módszerekkel, de) támogatott, despoták ellen harcoló szervezetek (vagy egy jó részük), gyakorlatilag a Nyugat ellen fordultak.[17] Ezért nem csak a támogatásukat vonták meg, de olyan feltételeket igyekeztek teremteni, amelyben ezen szervezetek (elsősorban az ISIS) felszámolhatókká váltak. Ennek kevésbé látványos eleme volt a pénzügyi folyamatok zárolása, de ide sorolható az iráni atomalku, amelynek folyományaként Irán közvetlen katonai erőkkel is kész és képes volt szembeszállni az ISIS erőivel szemben. Az oroszok beavatkozása nemzetközi hallgatólagos beleegyezés mellett történt. Az ISIS

[17] Megtudható az Edward Snowden által nyilvánosságra hozott, illetve az úgynevezett Wikileaks dokumentumokból.

elleni közvetlen harcok fő részese a kurd ellenállás, illetve a Szíriai Demokratikus Erők (Syrian Democratic Forces – SDF) kézi- és nehézfegyverekkel való ellátása mellett a légitámogatást is biztosította a Nyugat. Mindez vezetett el ahhoz, hogy már 2015-ben elkezdett csökkenni a nyilvántartott terrorcselekmények száma.



6. ábra: Menekültek főbb származási ország szerint 2010-2015 között

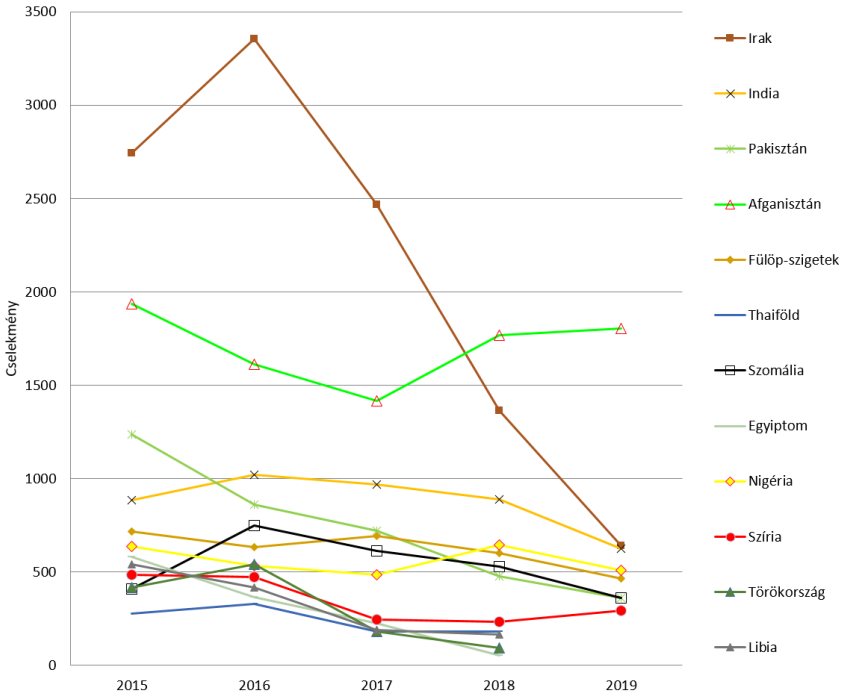
Az ún. „Arab tavasz" utáni fél évtized menekültügyi adatai lényegében nem támasztják alá azt a hipotézist, hogy azon országokból menekültek el a legtöbben, ahol drasztikusan megnőtt a terrorcselekmények száma (6. ábra). Legélesebb eltérés éppen Irak esetében látható, ugyanis, míg a vizsgált időszakban a terrorcselekmények itt ugrottak meg leginkább és a nagyságrendje is lényegében meghatározta a globális adatok súlyát és irányát, addig az innen menekülők száma drasztikusan csökkent (1,68 millióról 261 ezerre), és ezzel a világon regisztrált menekülteken belüli súlya is a korábbi (16,9%-ról 1,7%-ra) tizedére esett. Az afganisztáni menekültek száma a magas számuk mellett is inkább esett, mint stagnált. A terrorcselekményeknél említett hármas utolsó tagja, Pakisztán esetében ugyan az utolsó két évre (2014-15) megtízszereződött a menekültek száma, de a nagyságrendjük (300 ezer fő) még messze volt ahhoz, hogy érdemileg befolyásolja a globális trendet. Ezt lényegében egy másik országból menekülők adatai tették meg, amely nem más, mint Szíria. Érdekes módon, míg a terrorcselekmények száma ezen időszak alatt Szíriában ugyan tízszeresére nőtt, de a nagyságrendje még 2015-ben is „csak" megközelítette az 500 cselekményt, addig az innen elmenekültek száma szinte a nulláról lódult 5 millióra, így a globálisan regisztrált menekültek harmada ebből az országból került ki 2015-

ben. Ezzel lényegében ebből az egy országból származó menekültek száma és emelkedő trendje határozta meg a globális növekedést. Ami lényegében alá is támasztotta az innen menekülőkre irányuló médiafigyelmet.
Vagyis azt láthattuk, hogy Közel- és Közép-Kelet a meghatározó továbbra is mind a terror-, mind a menekültügyi eseményekben. Ez szorosan összefügg a nyugati beavatkozásokkal és be nem avatkozásokkal. Ami úgy is magyarázható, hogy a Nyugat bizonyos (be nem vallott) támogatása mellett induló „Arab tavasz" polgárháborús állapothoz vezetett, illetve a megszállt Irakban egyfajta „felszabadító" terrorhullám indult el a változásokat érzékelve. A menekültek számának stagnálása, enyhe csökkenése is részben ennek köszönhető, mivel többen reménykedtek, hogy kedvező változások következnek, ezért talán nem kell elmenekülni. Ezzel szemben Szíriában az erőszakosan fellépő Asszad-rezsim hamar kiábrándította a tömegeket abbéli reményükben, hogy megszűnhet a diktatúra, erre erősítettek rá az ISIS brutális fellépései, és generálták[18] a menekülthullámot. Vagyis alapvetően a terror indukálta a menekülthullámot, ha az adatok ezt nem is mutatják ilyen direkt módon.

Az utóbbi évek

Ahogy már az előző fázis elemzésénél láttuk 2015-ben már megindult egy csökkenő fázis, mivel 2014-ben követték el a legtöbb (regisztrált) terrorcselekményt, szám szerint 16.818-at. Ezután nem csak globálisan, de a legtöbb terrorcselekményt elszenvedő országok szinte mindegyikében érzékelhető a csökkenés. (7. ábra)

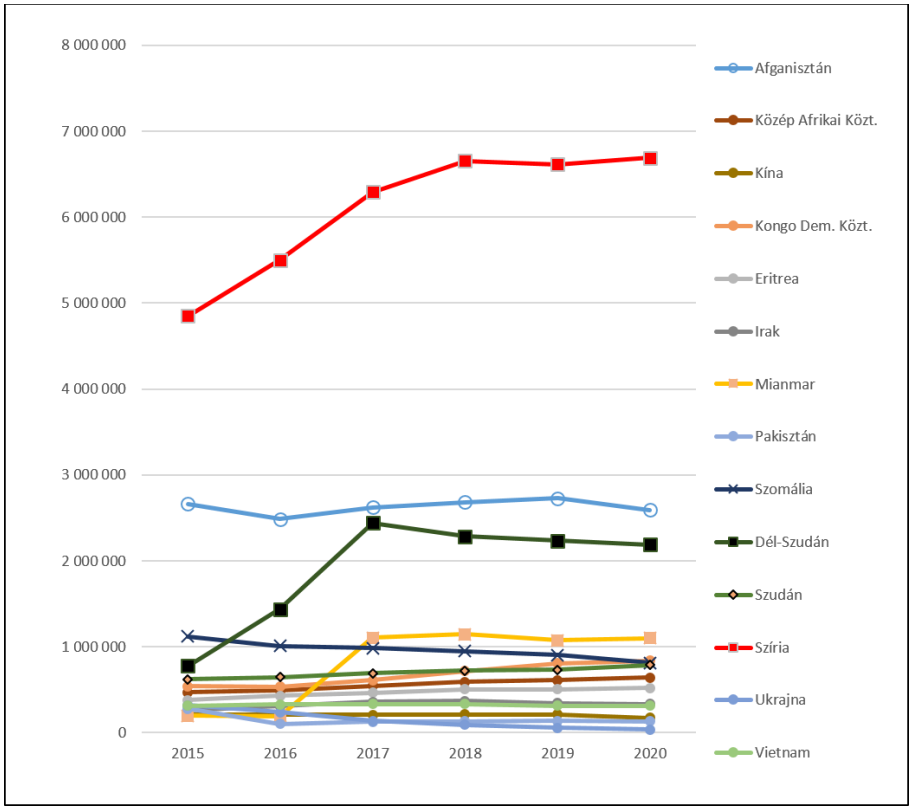
[18] Amelyet több egyéb ok is erősített, lásd RITECZ György: Az Európába irányuló tömeges irreguláris migráció felfutásának és megszűnésének okai; Hadtudomány, 2018/3-4. pp. 66-78.



7. ábra: Terrorcselekmények alakulása a legjellemzőbb országokban 2015–2019-ben[19]

A 7. ábrán is jól érzékelhető, hogy igazán meghatározónak a terrorcselekmények számában és ezáltal annak változásában is az Irakban elkövetett cselekmények számítanak még mindig. Vagyis azzal, hogy az ott 2016-ban elkövetett 3356 cselekmény 2019-re már majdnem a hatodára (642) esett. A globális csökkenést ez egyértelműen befolyásolta, ezt jelzi Irak összes cselekményen belüli aránya, amely 24,9%-ról 7,6%-ra esett. Közben a legtöbb terrorcselekmény helyszínét adó országok mindegyikében 30-50%-os esés is megtörtént. Lényegében egyedül Afganisztánban maradt ez időszakban tartósan évi 1500-2000 között a terrorcselekmények száma. Ami lényegében már utal arra is, hogy – az ISIS visszaszorítása ellenére – a közép-ázsiai térség továbbra is a legaktívabb a terrorcselekmények vonatkozásában. Ezt jelzi, hogy a nagymérvű csökkenések ellenére, illetve azokkal együtt is az ismert hármas (Irak, Afganisztán, Pakisztán), kiegészülve Szíriával, 2016-ban még a világon ismertté vált terrorcselekmények közel felét (46,8%) szenvedte el, de 2019-ben is még minden harmadik (35,9%) ilyen cselekményt ezen országokban követtek el.

[19] Ahogy már említettük, sajnos 2020-ra nem rendelkezünk GDT adattal.



8. ábra: Menekültek főbb származási ország szerint 2015–2020 között.[20]

A regisztrált menekültek száma lényegében stagnál az utóbbi években, ezt jelzik a „főbb" kibocsátó országi adatok is. Azzal együtt is, hogy 2018-ig még emelkedett a szíriai menekültek száma, ahogy a dél-szudániaké is (2017-ig),[21] a stagnálást érzékelteti, hogy a földön regisztrált összes menekült fele (50,8–47,9%) még mindig az ismert hármas (Irak, Afganisztán, Pakisztán) és Szíria polgárai közül kerül ki.[22] Vagyis e térség a meghatározó a terrorcselekmények és a menekülés szempontjából is. Tehát az elmúlt évtizedekben a nyugat által elindított demokratizálási, modernizációs szándék által gerjesztett folyamatok csődöt mondtak, gyakorlatilag működésképtelen államok alakultak ki az említett országokban, ahonnan, aki teheti, elmenekül.[23]

---

[20] Megjegyzendő, hogy 2019-ben 3,7 millió venezuelai is menekültnek minősülne, de őket az ENSZ is külön kezeli a statisztikákban, így nem kerültek a grafikonra.

[21] A Mianmari genocídium lényegében nem minősül terrorcselekménynek (az állam által elkövetett terror nem tartozik a fogalomkörbe), így ennek elemzésébe nem megyünk bele.

[22] Megemlíthető, hogy 2020-ban, a Covid19 folytán a nemzetközi határforgalom töredékére esett, ezzel együtt is a nemzetközi menekültek számszerűsége nem változott.

[23] Deák József: Az Oroszországi Föderáció határőrizeti kihívásai napjainkban. Hadtudomány 26. évfolyam 2016/E-szám, p. 7. URL.:http://mhtt.eu/hadtudomany/2016/2016_elektronikus/1_deak%20jozsef.pdf (Letöltés ideje: 2020.09.03.)

Ami mögötte van

Talán itt az ideje belátnunk, hogy a régi elv, mely szerint „az ellenségem ellensége a barátom", nem biztos, hogy még mindig, illetve minden esetben helytálló. Ugyanis ezen elv alapján kezdte támogatni az USA az afganisztáni ellenzéket a szovjet megszállás idején, majd ebből nőtt ki az Al-Kaida. Az „Arab tavasz" követően – mivel Aszad szír elnököt nem tudta megbuktatni az ellenzék – ismét nyugati támogatás érkezett, ennek lett „gyümölcse" az ISIS. Szomáliában már 1993-ban pórul jártak az amerikai fegyveres erők intervenciójuk során.[24] Nigériában pedig ott a Boko Haram, amelyet annak idején az Al-Kaida képzett ki és finanszírozott, majd hűséget fogadott az ISIS-nek. E szerint az elmúlt két évtizedben kialakult terrorhullámok, majd az ezt követő irreguláris migrációs hullámok alapvetően az ún. fejlett nyugat[25] lépéseinek következtében alakultak ki.

A vizsgált statisztikák (főleg az ismert „hármas" adatai) alapján talán kijelenthető, hogy a terrorcselekmények jelentős részben hozzájárulnak, hogy egyes országokban menekülni kelljen az embereknek.[26] De azt is látni kell, hogy más *(pull-push)* tényezők is közrejátszhatnak,[27] mivel számos ország esetében a magas terrorfenyegetettség sem indukál (statisztikailag érzékelhető) menekülést (például India, Fülöp-szigetek), míg más államok esetében magas menekülési adatok tapasztalhatóak annak ellenére, hogy az adott országban regisztrált terrorcselekmények száma[28] nem olyan kiemelkedő (például Eritrea, Koszovó). Ez is arra utal, amit már Maslow óta tudunk, hogy az ember cselekedeteit a szükségletei motiválják, de hogy a szükségletkielégítés útját-módját mi minden befolyásolhatta, azt a vizsgálatunk tárgyát képező időszakokban az „extrém" illegális migrációs hullámokban[29] érintetteknél tovább kellene elemezni, amelyre terjedelmi okokból nem térhetünk ki.

Ezzel együtt a migráns hátterűek közül néhányan követtek el súlyos terrorcselekményeket, amelyek a tömeges irreguláris migráció időszakában jelentős médiahátteret kaptak, és a civil lakosság szubjektív biztonság érzetére is jelentős hatást gyakoroltak. Ennek hátterében elsősorban – állítják a szociológusok[30] – az identitás elvesztése állhat. Ugyanis a másod- vagy harmadgenerációs migráns

---

[24] http://navyseals.hu/tortenelem/szomalia/a_mogadishui_csata.html (Letöltés ideje: 2015. 07. 18.)

[25] Ezen belül is elsősorban USA aktuálpolitikája befolyásolta ezeket a tevékenységeket.

[26] PETHŐ-KISS Katalin: Countering Terrorist Act Against Christian Places of Worship; Perspectives on Terrorism, 2020 June/XIV. pp. 75-88.

[27] Részletesebben lásd: RITECZ György: A tömeges migráció és/vagy népvándorlás ürügyén. A kialakult tömeges migráció katalizátorai; In: DEÁK József – GAÁL Gyula – SALLAI János (Szerk.): A toll sokszor erősebb, mint a kard; NKE Szolgáltató Kft., Budapest, 2016. pp. 174-189.

[28] Itt meg kell jegyezni, hogy azért a terrorcselekmények statisztikáinak megbízhatósága, pontossága is kérdéses lehet, ugyanis a terrorizmus kutatása és adatai igencsak „megismerési akadályokkal" terheltek. Lásd: BAKÓCZI Antal: Megismerési akadályok a terrorizmus kutatásában; Belügyi Szemle, 2015/7-8. pp. 88-105.

[29] DEÁK József: Határőrizeti és testületi modernizációtól a mai népvándorlás határrendészeti kezeléséig: a határrendészeti tisztképzés negyedszázada; Határrendészeti tanulmányok, 2017/2. pp. 70-79.

[30] http://hvg.hu/hvgfriss/2015.03/201503_muszlimok_dzsihadistak_es_rasszistak_europa (Letöltés ideje: 2015. 04. 02.)

muszlimok (azaz a bevándorlók leszármazottai, akik már valamely EU-tagállamban születtek, nőttek fel) bizonyos hányada – amilyenek a párizsi terror elkövetői is voltak – már nem érzi sajátjának szülei, nagyszülei kultúráját,[31] de az európai társadalmak sem fogadják be őket, és gyakori tapasztalatuk a diszkrimináció. Ebben a kitaszítottságban sokan fogékonyak a szélsőséges, internetes portálokon és egyes európai mecsetekben módszeresen hirdetett, gyújtó hangú ideológiákra, és csatlakoznak a közel-keleti dzsihádista mozgalmakhoz, vagy azok európai sejtjeihez. Mondhatnánk azt is, addig van szerencsénk, amíg elutaznak egyfajta „terrorturistaként", és valamely közel-keleti országban élik ki az identitászavarból fakadó frusztráltságukat. A kockázat abból fakadhatott volna, amikor visszajönnek szülőföldjükre, és ott akarnának terrorcselekményeket elkövetni. Ezen félelmek azóta szerencsére nem igazolódtak, közben a lakosság egy részében és a rendészeti szervekben aggodalom továbbra is jelen van ezzel kapcsolatban. Ugyanakkor nem tekinthető mindenki potenciális terroristának, aki abból a térségből érkezik. Ezért kell a nemzetbiztonsági szerveknek jól dolgozniuk, és még jobban együttműködniük a tagállamok biztonsági szerveinek,[32] sőt talán egy integrált, európai szintű titkosszolgálati szervre lenne szükség.[33] Ugyanis, amennyiben csak a hadsereggelés a rendészeti szervekkel kívánjuk feltárni és megoldani a terrorizmus által okozott kockázatokat, akkor a szabadság/biztonság tipikus dilemmájába ütközünk, és félő, hogy a biztonságunk (vagy legalábbis a vélt biztonságunk) érdekében a szabadságunk jelentős részéről mondunk le.[34]

Mindenesetre fontos, hogy a franciaországi és a belgiumi terrorcselekményeknek nem igazán a bevándorlás, sokkal inkább az integráció kérdésére kellene ráirányítaniuk a figyelmet. Az Európai Unió éppen a migrációs kérdések komplex módon való kezelésének elősegítse érdekében a 2007-2014-es pénzügyi időszakra létrehozta[35] és működtette az ún. szolidaritási alapokat.[36] A négy alap: Menekültügyi, Integrációs, Visszatérési és Külső Határok Alap, viszont a rendelkezésre álló forrásoknak általában csak kis része – országonként eltérő, 5-15%-a[37] – jutott az integrációs feladatok segítésére, ez pedig elgondolkodtató. A 2014-2020-as pénzügyi tervezési időszakban újabb struktúrában kerültek felhasználásra a migrációra és a belső biztonságra tervezett források. Egyrészt a Menekült és

---

31 A többség nem is tartja a vallását, a rítusokat, nem jár mecsetbe.

32 Részletesebben lásd: KOVÁCS Gábor: A migráció bűnügyi hatásai a magyar határrendészet kockázatelemzési rendszerére; In: HAUTZINGER Zoltán (Szerk.): A migráció bűnügyi hatásai; Magyar Rendészettudományi Társaság Migrációs Tagozat, Budapest, 2016. pp. 141-150., valamint: KOVÁCS Gábor: A rendőrség vezetésirányítási rendszerének sajátosságai a migrációs válsághelyzet kezelése során; In: TÁLAS Péter (Szerk.): Magyarország és a 2015-ös európai migrációs válság; Dialóg Campus Kiadó, Budapest, 2017. pp. 125-148.

33 A gyakorlat azt mutatja, hogy a prümi egyezmény a jó irányt jelölte ki, de az „önkéntes" jelleg már nem elégséges.

34 DEÁK József: A terrorizmus természete és az ellene történő fellépés nehézségei Oroszországban a Szovjetunió szétesésétől napjainkig; Belügyi Szemle, 2015/7-8. pp. 137-151.

35 European Commission Directorate-General Justice, Freedom and Security – SOLID/2007/27 – Committee General Programme Solidarity and Management of Migration Flows meeting 20 September 2007.

36 A szolidaritási alapok weblapja: http://solidalapok.hu

37 Magyarországnak a biztosított több mint 92 millió euróból kevesebb, mint 12,5 millió euró jutott erre a célra.

Migrációs Alap (MMA), másrészt a Belbiztonsági Alap (BBA) keretében, de az integrációra (az arányokat tekintve) ebben a ciklusban sem jutott több pénz.[38] A 2021–2027-es EU pénzügyi időszakban ismét változik a struktúra, a Menekültügyi, Migrációs és Integrációs Alap (AMIF – MMIA), a Határigazgatási és Vízumpolitikai Pénzügyi Támogatási Eszköz (BMVI – HAVE) és a Belső Biztonsági Alap (ISF)[39] keretében valósul meg a migráció kezelés EU-s támogatása. A tervezési feladatok a Covid19 miatt némi csúszásban vannak, de információk szerint az integrációra hazánk még az eddigieknél is kevesebbet tervez.

Eközben az idegenellenes hangulat(keltés)[40] éppenhogy provokál, és nem az integrációt segíti, hanem ellehetetleníti azt, sőt radikalizálni tudja a szélsőjobboldali és a szélsőbaloldali elemeket. Itt játszik szerepet a globalizáció egyik katalizátora, az új típusú média, ahol a „rémhír" mindenekelőtt áll. Holott a statisztikai adatok alapvetően nem támasztják alá azt a közvélekedést, hogy a globálisan jelentkező migráció, és az azon belüli, Európát érintő migrációs nyomás objektíve növelné a terrorcselekmények számát az öreg kontinensen. Ezzel együtt a szubjektív biztonság érzékelhetően csökkent. A kérdés valójában az, hogy ez miből eredeztethető, milyen tényezőknek köszönhető? Vélhetően számos szociológiai, szociálpszichológiai, de talán politológiai kutatás is szükséges ennek feltárásához. Mindenesetre az eddigi információk alapján kijelenthető: annak ellenére, hogy közel húsz évig[41] háborút folytattak az euroatlanti közösség[42] államai, a közemberek információs ingerküszöbét nem igazán érték el az erre vonatkozó hírek, információk mindaddig, amíg a harcok Ázsiában és Észak-Afrikában zajlottak, csak azt követően, amikor már egyes nyugat-európai államokban is megjelentek az ezen térségekhez közvetlenül, vagy közvetetten kapcsolódó terrorcselekmények.

Eközben a média, az emberek tájékozódása, értékválasztása is jelentős mértékben átalakult az internet gyors, olcsó elérhetőségének, a mobil- és okostelefonoknak és – nem utolsósorban – a média bulvárosodásának köszönhetően. Az emberek ilyen jellegű befolyásolhatósága megnövekedett, a nem megalapozott (hamis) információk is ugyanolyan gyorsan terjednek, a közösségi hálón keresztül elérhető (sok esetben torzult) információt nem ritkán megbízhatóbbnak vélik,[43] mint a (nehezen érthető, nem a közemberek nyelvén szóló) hivatalos kommünikét, vagy a tudományos eredményeket. Ez a politikai kommunikációra is rányomta a bélyegét, vagyis ahhoz, hogy a tömegeket befolyásolni tudja az adott politikai szereplő, neki is

---

38 Hazánkban a két alap forrásösszegének mindössze 15,02%-át tervezték integrációs feladatokra. Bár a Covid19 miatt gyakorlatilag még mindig nem zárult le teljesen a projekt időszak, de úgy tűnik, még a tervben szereplő finanszírozás is csak részben valósult meg.

39 http://belugyialapok.hu/alapok/2021-2027 (Letöltés ideje: 2022. 03. 25.)

40 Az idegenellenességről lásd bővebben: GÖRBE Attiláné ZÁN Krisztina: „Mi" és „ők". Migráció és idegenellenesség a társadalmi megítélés tükrében; DOBÁK Imre (Szerk.): Szakmaiság, szerénység, szorgalom; Dialóg Campus Kiadó, Budapest, 2018. pp. 241-251. ISBN: 978-615-5889-51-6, valamint: GÖRBE Attiláné ZÁN Krisztina: Nemzetközi xenofóbia kutatások; In: DEÁK József – GAÁL Gyula – SALLAI János (Szerk.): A toll sokszor erősebb, mint a kard: rendészettudományi tanulmányok Prof. Dr. Fórizs Sándor 65. születésnapja tiszteletére; 2016. pp. 84-100. ISBN: 9786155527982

41 2001. 09. 11.

42 Neve ellenére nem igazán viselkedik közösségként, ezért sem tudja hatékonyan kezelni problémáit.

43 Sok esetben a GPS-nek is jobban hisznek az emberek, mint a saját szemüknek.

ezt a (populista, demagóg) stílust, technikát kell alkalmaznia. Ez jól érzékelhető volt akár a 2016-os amerikai elnökválasztás kapcsán is, ahol Donald Trump jelöltségére, majd megválasztására racionálisan szinte senki sem fogadott volna a jelöltállítási folyamat kezdetén, de idesorolható a Brexit-népszavazás is, amikor a logikus érvek alulmaradtak a féligazságokkal szemben. Nem véletlen, hogy a Brexit kulcsszemélyei milyen hamar visszaléptek az EU-ból való kivezető út levezénylésétől. Ez is jelzi, hogy csak a rövid távú érdekek a lényegesek, a hosszabb távú stratégia, előretekintés már nem divat. Ezt sugallja valamennyi médiafelület, a fogyasztói társadalom, amely egyfajta identitás- és értékválságot[44] is generál. Mintha az érzéki észlelés kerülne egyre inkább előtérbe az intellektuális helyett, vagyis az emberek egy jelentős része egyre inkább ösztönlényként[45] ténykedik. Ez viszont felerősítheti a felettes én befolyását, és teret enged a tekintélyuralmi rendszerek térhódításának. Mint tudjuk, *„a tömegben milyen erős vágy él a tekintély után, melyet csodálni lehet, mely előtt meghajolhat, amely uralkodik rajta…"*[46] Talán ezt jelzi például Vlagyimir Putyin, Recep Tayyip Erdogan, Hszi Csin-ping, Abdel-Fatták esz-Szíszi helyzete, és még folytatható a sor. Felmerülhet a kérdés: a helyzet miatt változott a „vezetési stílusuk", vagy ők teremtettek olyan helyzetet, hogy „egyeduralkodóvá" válhassanak?

A közvélekedés alakulásában az is szerepet játszhat, hogy hogyan dolgozzák fel a fejlett nyugati társadalmak és polgáraik azt a felelősséget, amely legalább részben terheli őket a terror helyszínévé és egyúttal migráció-kibocsátóvá váló országok instabillá tételében. Vagyis azok, akik felelősséget éreznek az államuk vezetői által tett,[47] illetve tenni elmulasztott[48] intézkedések miatt, egyfajta bűntudatból is, megértőbben viszonyulhatnak a migránsokhoz, pontosabban a menekülőkhöz. Viszont azok, akik ezt a felelősséget nem látják, vagy nem akarják tudomásul venni, egyfajta kognitív disszonancia velejárójaként – én/mi jók vagyunk, nem követtünk, nem követhettünk el hibákat, bűnöket – magát a migrációt, illetve az irreguláris migránsokat tekintik a bajok forrásának. Az nyilvánvaló, hogy a menekülők ideális alanyai a bűnbakképzésnek,[49] hiszen nem beszélik a nyelvünket, másként öltözködnek, más a vallásuk, más kultúrkörhöz tartoznak, tehát nem „mi vagyunk". A 2008-as elhúzódó[50] gazdasági válság vesztesei, illetve a gazdasági élénkülést a mindennapi életükben nem érzékelők körében viszonylag könnyen megfogan a gondolat, hogy minden baj okozója a migráció és maga a migráns. A projekció (kivetítés) nemcsak a gazdasági fejlődés elmaradásától való félelemre, a munkahelyféltésre terjed ki, de akár az Európai Unió lehetséges szétesésének okozójává is minősíthetik, vagy akár járványok (Covid19) terjesztőiként is

---

44 *„Most viszont azt látják, hogy nem a szorgalmasok boldogulnak, hanem azok, akik megfelelő kapcsolatokkal rendelkeznek."* Lásd: DEÁK József – GAÁL Gyula – SALLAI i. m. p. 10.

45 Lásd például FREUD, Sigmund: Mózes; Európa Kiadó, Budapest, 1987. és CSÍKSZENTMIHÁLYI Mihály: A fejlődés útjai. A harmadik évezred pszichológiája; Nyitott Könyvműhely, Budapest, 2007. műveit.

46 FREUD, Sigmund: Mózes; Európa Kiadó, Budapest, 1987. p. 169.

47 Például: háborúk indítása, bombázások, háborús jogsértések börtönökben (Abu Ghraib)

48 Például: a be nem avatkozás egyértelműen embertelen és emberiség elleni bűncselekmények, háborúk és polgárháborúk esetében.

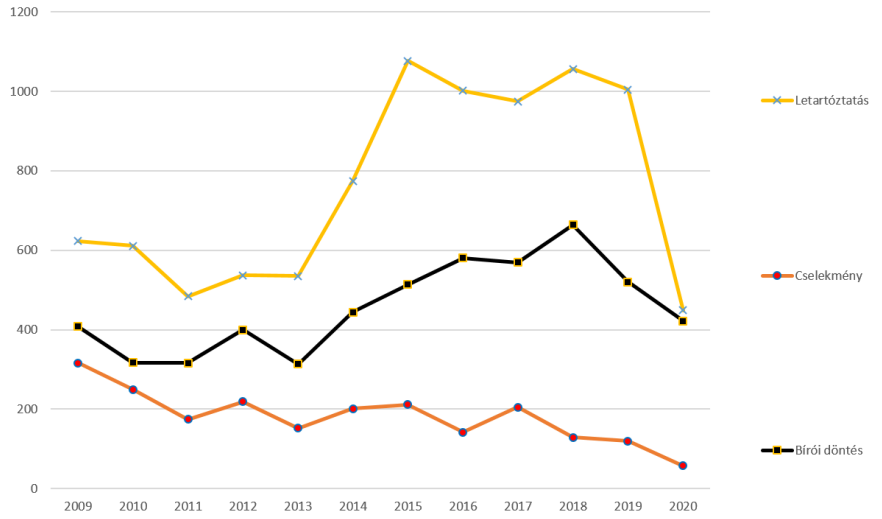
49 *„A populista mozgalmak középpontjában a bűnbak áll."* Lásd: BEN-AMI, Slomo: Demagógok múltja és jövője; HVG, 2016. 08. 18. p. 73.

50 Adatok alapján 2012-13-ig is eltartott, vagyis közel kétszer annyi ideig, mint a „nagy gazdasági világválság" (1929-32).

bélyegezhetik a migrációs folyamatban részt vevőket. Ezt a hárító mechanizmust és félelemkeltést sikeresen lovagolja meg a politikán kívül a média is.

Európában

Annak vizsgálata, hogy hogyan változott a terrorfenyegetettség Európában az elmúlt években, talán úgy a legautentikusabb, ha az EUROPOL terrorizmussal kapcsolatos jelentéseit[51] vesszük elő.



9. ábra: A terrorcselekmények és az azokkal kapcsolatos letartóztatások és bírói döntések száma Európában

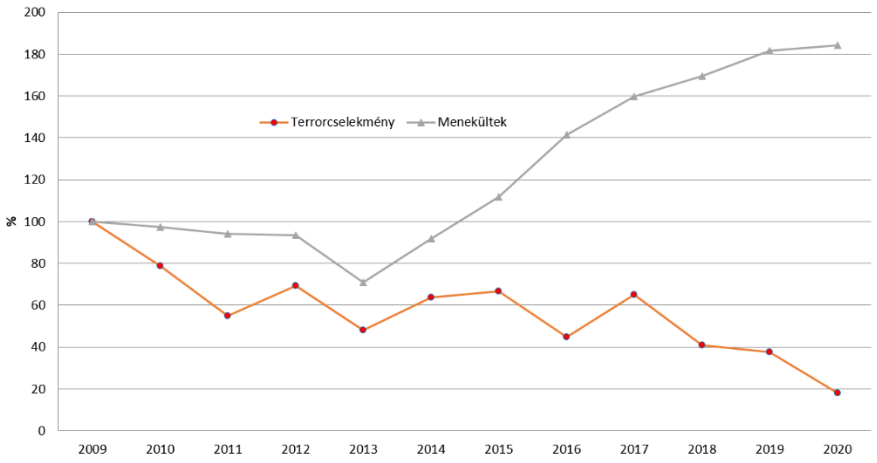
Tekintettel arra, hogy a migráció/menekültek és a terrorizmus kapcsolata igazán az utóbbi években lett a közbeszéd tárgya, elsősorban a Charlie Hebdo, Bataclan, illetve a nizzai és a belgiumi, németországi terrortámadások kapcsán,[52] ezért lényegében csak az utolsó évtized adatait nézzük meg. Az EUROPOL adataiból egyértelmű és folyamatos csökkenés látható az elkövetett terrorcselekmények számát tekintve. A 8. ábrán is látható, hogy a korábbi (2009) 316 terrorcselekmény helyett 2019-ben már ennek csaknem a harmadát (119 eset) követték el. Sőt, a letartóztatások száma is csökkenő tendenciát jelzett 2013-ig, aztán ez a szám 2014-ben 774 fő, 2015-ben pedig már 1077 fő, és ez az érték öt évig meg is maradt, majd 2020-ban visszaesett (erre még kitérünk). Bár mindehhez hozzá kell tenni, hogy ezek nem bizonyított esetek miatti elítélések, hanem csak valamilyen (remélhetőleg megalapozott) gyanú alapján történt letartóztatást takarnak. A téma átpolitizáltsága nemegyszer rányomja a bélyegét a jogalkalmazók tevékenységére, így ebben az esetben is talán erre utalhat

[51] Forrás: www.europol.europa.eu

[52] ALMADI Sejla: A bevándorlással kapcsolatos francia közvélemény 2012 és 2017 közötti alakulása; KKI-tanulmányok, a Külügyi és Külgazdasági Intézet időszaki kiadványa, T-2018/05.

az „eltérő trend”. Ha megnézzük a jogerősen lezárult bírói döntések számát, akkor is azt láthatjuk, hogy 2013 és 2018 között duplázódás történt. Talán nem véletlen az sem, hogy éppen 2015-ös évben emelkedett meg ötszáz fölé (514) a bírói döntések száma, éppen akkor, amikor a tömeges irreguláris migráció jellemezte Európát, miközben a ténylegesen elkövetett terrorcselekmények száma nem nőtt. Azt is érzékeljük, hogy közel kétszer annyi a letartóztatott, mint akik végül bíróság elé kerültek. A bírói döntésekről azt is tudni kell, hogy ezen esetek 20–30%-a felmentéssel végződik, illetve gyakran az ítélet sem terrorcselekmény miatti, hanem más bűncselekményekre vonatkozik. Feltűnő a letartóztatottak számának felére csökkenése 2020-ban. Ez alapvetően abból ered, hogy Nagy-Britannia (GBR) kilépett az Európai Unióból és így az uniós statisztikákból is kikerültek az adataik. Ezzel együtt, meg kell említeni, hogy GBR nélkül 2018-ban 783, 2019-ben 723 letartóztatás született, így a 2020-as 449-es érték azt jelzi, hogy az utóbbi időben már csökkenhetett, vagy akár meg is szűnhetett a politikai nyomás, a külföldiek terrorcselekmény elkövetésével való meggyanúsítás miatti letartóztatását illetően. Ugyan erre utal a bírói döntések számának GBR nélküli alakulása is (2018 – 549, 2019 – 520, 2020 – 422). Míg eközben a regisztrált terrorcselekmények száma jóval enyhébb mértékben csökken, illetve stagnál (2018 – 69, 2019 – 55, 2020 – 57).

A terrorcselekmények és a menekültstátuszt kapottak között feltételezett összefüggést a statisztikai adatokban talán az arányváltozások vizsgálatával lehet a legegyszerűbben szemléltetni. Éppen ezért a 2009-es év adatait tekintettük 100%-nak, és az ehhez képest történő változást vizsgáltuk (bázis index) és érzékeltetjük a 10. ábrán.



10. ábra: Az Európában elkövetett terrorcselekmények száma és a regisztrált menekültek számának változása 2009-hez viszonyítva (2009=100%)

Az adatok alapján kijelenthető, hogy míg az érkező irreguláris migránsok, illetve menedékkérők aránya egyre nagyobb Európában, addig a terrorcselekmények, illetve azon személyek száma, akik „jó okkal” ilyenek előkészítésével gyanúsíthatóak, egyértelműen csökkenést mutat (10. ábra). Ahogy az EUROPOL fogalmaz: *„A mai*

napig nincs konkrét bizonyíték arra, hogy a terroristák utazásaik során rendszeresen kihasználták volna az Európa felé irányuló tömeges migrációt."[53] Európában a terrorfenyegetettség nem is igazán a „bevándorlókhoz" köthető, hanem alapvetően a „bennszülöttekhez",[54] és csak kisebb részben a migráns hátterűekhez. A hosszabb távú trend még azt sem igazolja, hogy az egyre több „migráns"/menekült jelenléte egyre több szélsőjobboldali terrorcselekményt indukálna.[55] Igaz, hogy 2018-ban 44 fő volt a szélső-jobbhoz köthető terrorcselekmény miatt letartóztatottak száma, amely adat a 2015 évi 11-ről fokozatosan emelkedett, de 2014-ben is már 34 főt regisztráltak, sőt 2007-ben szintén pont 44-et, illetve 2019-ben már „csak" 21 főt, igaz 2020-ban ismét 34 főt, de ez is csak az összes ilyen cselekmény miatt letartóztatottak 7,6%-a. A szélsőjobboldal által elkövetett terrorcselekmények száma is csökkenő trendet mutat, a 2015-es 9 esetről 2020-ban 4 cselekményre mérséklődött a számuk.

Szélsőségek

Ahogy azt korábban említettük, napjaink globalizálódó világának sajátossága, hogy a társadalmi viszonyok rendkívül gyorsan változnak, és a média a korábbinál nagyobb felületen és hatásfokkal formálja az emberi tudatot. A globalizáció sajátos eredménye az is, hogy a közlekedés és a távközlés gyorsulásának köszönhetően az emberek viszonylag gyorsan és nagy létszámban tudnak helyet változtatni. A gyors földrajzi helyváltoztatás lehetőségének köszönhetően a számos társadalmi konstrukció is átalakuláson megy keresztül, például bizonyos térségekben az országhatárok szimbolikusabbá válnak, és a nemzet, és egy területegységhez kapcsolódó közösség fogalmának társadalmi értelmezése is változási folyamaton megy át. Természetesen ezen fogalmak változásának ténye mindig csak utólag állapítható meg igazán. Az egyének globalizációhoz és annak egyik kísérőjelenségéhez, a migrációhoz való viszonyulásának széles skálája van. Az egyik jelenséghez való viszonyulás erősítheti a másik jelenségről alkotott véleményt, vagy épp gyengítheti azt. A véleményalkotást formálhatják a személyes tapasztalatok, az egyén környezetének véleménye, a vallási és világnézeti beállítódások, és negyedik hatalmi ágként a média. Természetesen az egyéni attitűdöt nagyban meghatározza, hogy az egyén a fogadó társadalom tagjaként vagy migrációs hátterűként szemléli ezt a folyamatot. Mint minden társadalmi folyamathoz, így a migráció folyamatához is kapcsolódnak szélsőséges nézetek a fogadó társadalom és a migrációs hátterűek részéről egyaránt. A migrációhoz kapcsolódó szélsőséges attitűdökön kívül számos politikai és vallási természetű szélsőséges megnyilvánulás tarkítja az egyes országok közvéleményét.

Természetesen fontos kérdés, hogy ki számít szélsőségesnek. Ennek a meglehetősen szubjektív kérdésnek a megválaszolásában elsősorban az adott ország politikai vezetése az illetékes, ez különösen akkor fontos, mikor a szélsőséges szervezetek kezelésében illetékes rendészeti szerveknek ad instrukciót a szélsőségesek kezelésével kapcsolatban. Természetesen adja magát az értelmezés, hogy szélsőségesnek tekinthetők azok a csoportok és az egyének, akik az érvényben

---

53 EUROPOL TE-SAT 2020. p. 15. – a szerzők fordítása.

54 Például Anders Behring Breivik.

55 HAUTZINGER Zoltán: A terrorizmus elleni küzdelem idegenjogi eszközei; In: GAÁL Gyula – HAUTZINGER Zoltán (Szerk.): Pécsi Határőr Tudományos Közlemények, 2015. Pécs, p. 203.

lévő törvények és társadalmi normák betartásához szélsőségesen viszonyulnak. A szélsőséges viszonyulás szintén nehezen meghatározható. Egyfajta megközelítésben, a szélsőséges elkövetői attitűd motivációjával rendelkező bűncselekményt elkövető egyén vagy a csoport, a bűncselekményt követően szélsőségesként kerüljön besorolásra. Ez a szemlélet viszont csak korlátozottan adna lehetőséget a preventív fellépésre és a témához kapcsolódó rendészeti tevékenységre, ezért a politikai vezetés iránymutatása megkerülhetetlen. A politikai vezetők felelősségteljes iránymutatása és fellépése azért is fontos, mert a naprakész információkon alapulva, megfelelő politikai lépésekkel a szélsőséges csoportok társadalmi támogatottsága korlátozható, és a radikalizációs folyamatokat könnyebb korlátozni.

A migrációhoz kapcsolódó szélsőséges megnyilvánulások kapcsán fontos, hogy a befogadó társadalomhoz és/vagy a migrációs hátterűekhez kapcsolódó szélsőséges magatartást elemezzük. Mindkét szélsőséges oldalt érintik a radikalizációs folyamatok, amelyeknek löketet adhat a migráció.

Napjainkban a radikalizáció kutatását célzó szakirodalom noha kimondja, hogy a radikalizáció minden egyén esetében eltérően zajlik, viszont a rendészeti munka megköveteli, hogy a tudományos oldalról is kutatva legyen, hogy melyek a radikalizációs folyamat jelei és miként lehet ellene fellépni, és a radikalizációs folyamatban mikor kell preventív módon beavatkozni.

Természetesen a radikalizációs folyamatok és annak társadalmi kitettsége országonként és kultúrkörönként eltérő, így minden országnak saját monitoring rendszert kell kifejlesztenie és azt az aktualitások mentén folyamatosan frissítenie. Ugyanakkor természetesen más országok jó gyakorlata (best practice) formálni tudja az egyes országok rendészeti tevékenységét. Migrációs helyzettel kapcsolatos radikalizációs folyamatok kezelésére jó példát jelenthet Németország, ahol a szélsőséges csoportok kezelésén több rendészeti feladatot ellátó intézmény dolgozik. A szélsőségesek felosztása valamennyi illetékes rendészeti szervnél egységes terminológiát követ. A szélsőségeseknek négy fő csoportja van: a szélsőjobboldal, szélsőbaloldal, vallási ideológia, és a külföldi ideológia, vallási ideológia nélkül. Ez a kategorizálás 2017-től van érvényben, amikor feltehetően a 2015-ös tömeges irreguláris migrációs válsághelyzet miatt is, a korábbi külföldi kontextusú politikai motivált bűncselekmények kategóriáját kettébontották: a vallási ideológia által motivált bűncselekmények csoportjára és a külföldi ideológia vallási ideológia nélkül motivált bűncselekmények csoportjára. Ezen kategóriák bűnözési statisztikáira és annak elemzésére ebben a tanulmányban nem kívánunk kitérni, viszont ezen kategóriák alkalmasak arra, hogy szemléltessük a migráció egyes szélsőségekre gyakorolt hatásait.[56]

A szélsőjobboldal szemében a migráció növeli azoknak a számát, akiket nem tekintenek a nemzet részének, így az ellenük való fellépés aktivizálhatja az ide tartozó

[56] Szövetségi Bűnügyi Hivatal: Politikailag motivált bűncselekmények – szövetségi adatok. Wiesbaden, 2021. p. 3. https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/210504_PMK2020.html (Letöltés ideje: 2022. 02. 25.)

csoportokat. A szélsőjobboldali csoportok célkeresztjébe kerültek a migrációs hátterűek mellett a migrációt támogatónak vélt politikusok és médiumok is.[57]

A szélsőbaloldal a migrációs hátterűekben elnyomottakat és potenciális harcostársakat lát, akikkel együtt harcolhat a társadalmi rend átalakításáért, és akiket megszabadíthat az elnyomó politika alól. Sajátos német jelenség, hogy a németországi gyökérrel rendelkező baloldaliak tudnak kapcsolódni a külföldi baloldali csoportokhoz, amelyekkel számos közös tüntetést bonyolítottak le, illetve egyes német baloldaliak részt vettek a szintén baloldali ideológiát valló törökországi PKK (Partiya Karkerên Kurdistan − Kurdisztáni Munkáspárt) harcaiban fegyveresen, Törökországban és Szíriában.[58]

A migrációval kapcsolatban fennállhat véleménykülönbség a jobboldali és baloldali csoportok között, mely többször megnyilvánult a németországi tüntetéseken akár fizikai erőszak formájában is. Természetesen a két csoport közötti ellentéteket a politikai vezetés ügyes politikával fékezni tudja, viszont, ha gyakorlati összeütközésre kerül sor, akkor rendészeti szerveknek kell a különválasztásukról gondoskodnia. Ennek a folyamatnak sajátos tényezője, hogy a témához kapcsolódó rendészeti tevékenység meglehetősen speciális: a szakmai módszereket folyamatosan frissíteni kell, és hangsúlyt kell fektetni az állomány megfelelő (többek között pszichés) felkészítése. Ezt a munkát nehezítheti, hogy a rendészeti és a politikai szemlélet számos ok miatt eltérhet egymástól, és a szélsőségekhez való politikai hozzáállás változhat egy adott új kormány megalakulásakor. Ezen tényezőknek köszönhetően a rendészeti munkát végző állomány esetében is fennáll a veszély, hogy radikalizálódik. Ennek megelőzése miatt kulcskérdés a belső ellenőrzés. A belső ellenőrzés ikonikus példáját láthattuk Németországban, mikor valamennyi rendészeti szervnél ellenőrzést végeztek a szélsőjobboldali ideológia felé elhajlás kiszűrésének szándékával. Ennek az ellenőrzésnek az eredményét publikálták is.[59]

A vallási ideológiai motivációval rendelkező kategóriába tartozik az iszlamizmus mellett az összes olyan vallás, amelynek valamelyik csoportja a szélsőséges irányba mozdul el. Természetesen ebben a kategóriában az iszlamizmus a domináns, de például a hindu és a szikh kisebbségek, egyes szélsőséges keresztény valláshoz köthető csoportok is ide tartozhatnak. A vallási ideológiához tartozók körében a migráció és az arra való reagálás egy központi téma lehet. A migráció mellett számos egyéb tényező indíthat el egyéneket a vallási szélsőségek irányába, a migrációs kiinduló térségben gyakorolt vallás további gyakorlása csak egy a sok tényező közül. Természetesen a migrációhoz valamilyen módon kapcsolódó

---

57 Szövetségi Alkotmányvédelmi Hivatal kompendiuma: az egyes szakterületek és megfigyelési objektumok bemutatása. Köln, Szövetségi Alkotmányvédelmi Hivatal, 2018. pp. 13-39. https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/allgemein/2018-12-kompendium-des-bfv-darstellung-ausgewaehlter-arbeitsbereiche-und-beobachtungsobjekte.html (Letöltés ideje: 2022. 02. 23.)

58 Uo. pp. 39-61.

59 Szövetségi Alkotmányvédelmi Hivatal: Helyzetjelentés - jobboldaliak a rendészeti szerveknél. Köln, Szövetségi Alkotmányvédelmi Hivatal, 2020. https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/rechtsextremismus/2020-09-lagebericht-rechtsextremisten-in-sicherheitsbehoerden.html (Letöltés ideje: 2022. 02. 23.)

valláshoz köthető radikalizáció során nem ritkán az egyes generációk között különbség van. Az első generációsok körében a közvetlen migrációs tapasztalatot követően (a vallási gondolkodás továbbvitele esetén) a vallás biztosíthatja és erősítheti az egyén lelki hátországát, a kiinduló országhoz és annak társadalmához való kötődését. A migráció célterületén való beilleszkedési nehézségek, a társadalmi környezet változása, a migrációt elindító vágyak be nem teljesülése elindíthat egy szoros valláshoz való kötődést, amely könnyedén elmehet szélsőséges irányba is. Ezt a radikalizációs folyamatot segíthetik a korábban említett radikális nézeteket valló és terjesztő vallási vezetők. Emellett gyorsíthatták a radikalizációs folyamatot a kiinduló térségben lejátszódó kedvezőtlen társadalmi folyamatok, harci cselekmények, amelynek során a migrációs hátterű és/vagy családja vesztesnek érzi magát. A másod- vagy harmadgenerációsok körében általában már nincs közvetlen kapcsolat a kiinduló térséggel, ugyanakkor számos ok miatt jöhet létre olyan szituáció (identitáskeresés, kitaszítottság érzése), amikor az élet bizonyos kérdéseire a vallásban keresik a választ. Meg kell jegyezni, hogy a vallás felé fordulás még önmagában nem jelent radikalizációs folyamatot és a radikális vélemény befogadása nem jelent szükségszerűen terrorcselekmény végrehajtására vonatkozó motivációt.[60] Természetesen a többségi társadalom részéről is előfordulhat, hogy a migrációs hátterűek felé táplált ellenszenvüket vallási elemekkel is megtámogatva próbálják legitimmé tenni.

Meghatározó tényező a migrációs folyamatok által tarkított társadalmakban, hogy a különböző ideológiát valló szélsőséges társadalmi csoportok egymás radikalizációját is gerjesztik. Tehát az egyes társadalmi csoportok ellenségképként való feltüntetése, az ellenségként feltüntetett csoportok fenyegetettségérzetét növeli, így tovább eszkalálhatja a szélsőségek közötti feszültséget.[61] Emellett a szemben álló csoportok közötti feszültség erősödése bevonzhat újabb szereplőket a konfliktusba belföldről és külföldről is. Belföldi konfliktus eszkalálódására példát jelenthet, amikor a migrációs hátterűek és a szélsőjobboldal közötti konfliktushelyzetben a társadalmi egyenlőségért folytatott harc jegyében a szélsőbaloldal megjelenik a migrációs hátterűek oldalán,[62] így a meglévő konfliktus tovább eszkalálódásának veszélye állhat fenn. A szélsőségesek közötti konfliktusokba való külföldi beavatkozásra példát jelenthet, mikor a belföldi konfliktusok élezésében külföldi szereplők is aktívan szerepet játszanak. Ennek szomorú példája a korábban említett szélsőséges vallási közösségek létrejöttének támogatása külföldről érkezett vallási vezetőkkel, hitszónokokkal, közösségi terek építésével.[63]

Nyugat-Európa országaihoz hasonlóan Németországban is van tere a különböző kultúrkörből és etnikai csoportból érkező migrációs hátterű csoportok közötti − a migráció kiinduló térségeiből magukkal hozott társadalmi csoportok közötti ellenétekből eredő − feszültségek folytatására és továbbéleződésére a migráció

---

60 BÁCS Zoltán György: A radikalizáció és a terrorizmus kapcsolata, egyes formái, gondolatok a megelőzés lehetséges perspektíváiról; Nemzetbiztonsági Szemle, Budapest, 2017/1. http://epa.oszk.hu/02500/02538/00017/pdf/EPA02538_nemzetbiztonsagi_szemle_2017_01_005-026.pdf (Letöltés ideje: 2022. 02. 23.)

61 ROSTOVÁNYI Zsolt: Iszlám, migráció, terrorizmus. ezredveg.vasaros.com/, 2016. (Letöltés ideje: 2022. 02. 27.)

62 Ezt mutatják a TE-SAT jelentések is, illetve lásd: SUHAJDA Attila: Politikailag motivált bűnözés és a migráció kapcsolata Németországban 2014 és 2020 között tanulmányát.

63 Szövetségi Alkotmányvédelmi Hivatal kompendiuma i. m. pp. 61-99.

célterületén, vagy a tranzitországokban. Ezen szélsőséges csoportok közötti viszonyrendszert erősen befolyásolják a kiinduló térségben történt események, az ottani viszonyrendszerek, és ezeknek a migrációs célországban lévő diaszpóra társadalmában való manifesztálódása.[64]

A szélsőséges csoportok létrejötte értelmezhető a társadalmi integráció kudarcának, viszont a helyzet ennél bonyolultabb. Természetesen igaz, hogy a szélsőséges társadalmi csoportok elkülönülésének lehetőségéért érdemes kritikával illetni a fennálló társadalmi viszonyokat, viszont rendkívül nehéz annak az alapvető emberi attitűdnek gátat vetni, amelynek alapján az egyén olyan társaságot keres, amellyel vannak közös pontjai, és jól tudja érezni magát. Ebből az állításból következhet az is, hogy a sikeres társadalmi integráció egyik fő feladata, hogy a különböző etnikai és szociális hátterű csoportokat egymáshoz fizikailag és szellemileg közelebb hozza. De látni kell ennek a megfontolásnak a nehézségeit és korlátait. Rendkívül nehéz egy szegregációs folyamatban benne lévő egyént, és a sok esetben az ismeretlentől félő, nem migrációs hátterű egyéneket tartósan közelebb hozni egymáshoz.[65] Emellett rendkívül nehéz ellensúlyozni azt a korábban említett politikai magatartást, amely a társadalmi problémák megoldása helyett bűnbakképzéssel és a hozzákapcsolódó megmentő szereppel kíván társadalmi szimpátiát szerezni.[66] Az ehhez kapcsolódó politikai kommunikáció tovább mélyítheti az egyes társadalmi csoportok közötti feszültséget, és nagyban csökkentheti a társadalmi integrációt célzó intézkedések hatékonyságát. Természetesen a migrációs hátterűek egy részénél is előfordulhat a társadalom másik felének démonizálása és egyoldalú megítélése, amely szintén elősegíti a radikalizálódást. Az egymásról kialakított vélemények közvetítésének legfontosabb eszköze lehet a média (ezen belül egyre nagyobb teret nyer a közösségi média), amelyen keresztül gyorsan lehet pozitív és negatív irányba formálni a közvéleményt társadalmi kérdésekben is.[67]

Ezen kívül a radikalizációnak egyre gyakrabban előtérbe kerülő változata, mikor a radikalizálódásnak egyik ideológia sem adja hozzá a szellemi támogatást. Ilyenek például a családi vagy egyéb életkörülménybeli nehézségek (pld. iskolai, munkahelyi) miatt utcán, munkahelyen, vagy éppen az otthonaikban agresszív cselekedeteket elkövetők, akiket nem sikerül a nyomozás végén sem valamelyik ideológia által motivált elkövetési kategóriába sorolni.[68]

Szintén bonyolult kérdéskör, hogy a megkezdődött radikalizációs folyamatot meg lehet-e száz százalékosan állítani, és az újrakezdődését meg lehet-e gátolni? Természetesen bárhogy is válaszolja meg az előbbi kérdéseket a témával foglalkozó szakirodalom, akkor is meg kell próbálni eltéríteni a társadalmilag elfogadhatatlan útra tévedt embereket, eltántorítani a terrorcselekmények elkövetésétől. Persze ez

---

64 Szövetségi Alkotmányvédelmi Hivatal kompendiuma i. m. pp. 99-119.

65 BIZEUL, Yves – RUDOLF, Dennis Bastian: Politikai viták a migráció és integráció körül: koncepciók és esettanulmányok; Springer Kiadó, Wiesbaden, 2019.

66 BRECHER, Philippe – BEGASS, Christian – KRAFT, Josef: A mélység előretörése–AfD, Pegdida társai: a szalonoktól az utcáig; Pappy Rossa Kiadó, Köln, 2015.

67 ANTAL Zsolt – GAZSÓ Tibor – KUBINYI Tamás – PELLE Veronika (Szerk.): Médiabefolyásolás – Az új kislexion. Századvég Kiadó, Budapest, 2015.

68 Például Bajor Médiatéka: München- egy város félelemben (dokumentumfilm), München, 2019. https://www.br.de/mediathek/video/dokumentarfilm-muenchen-stadt-in-angst-av:5b1661554c4c850018cabc5f (Letöltés ideje: 2022. 02. 22.)

rendkívül nehéz, amikor a rossz útra tévedt egyén ebben nem akar részt venni, vagy csak színleli az együttműködést, mint ahogy a 2020. novemberi bécsi támadás elkövetője is tette.[69] A sikeres deradikalizációs folyamat, és általában a társadalmi integráció komoly anyagi és humánerőforrást igényel, amelyet nem könnyű előteremteni, hiszen annak sikeres működése esetén „csak" a normál társadalmi működés feltételeinek megteremtése zajlik, amely ritkán találkozik a profitot előtérbe helyező társadalmi és politikai szemlélettel.

Befejezés

Összegezve megállapítható, hogy a terrorizmus és a nemzetközi migráció között van kapcsolat. Viszont ez a kapcsolat térségenként, országonként és időszakonként is változik, és változott a kétpólusú világrend megszűnését követően. A terrorizmus kétségkívül az egyik leglátványosabb és legszörnyűbb push-faktora a nemzetközi migrációnak, viszont nem szabad figyelmen kívül hagyni a többi push- és pull-faktort sem. A terrorizmus és a migráció nemzetközi tendenciáit elemezve látható, hogy az elmúlt évtizedben a terrorizmus és migráció/menekülés jelentős mértékben koncentrálódik a válságkörzetekre, és egy-egy ország kiemelkedő adatokkal és/vagy növekvő tendenciával rendelkezik. Természetesen a két jelenség számadatainak elemzésére, így a következtetések levonására is hatással van, hogy milyen mutatókkal vizsgáljuk meg, és az adatok milyen módszertan mentén kerülnek gyűjtésre és elemzésre. Mindkét jelenségre jellemző, hogy kiváltó okai igencsak összetettek, és a kezelése rendkívül bonyolult dolog, amely nem nélkülözheti a nemzetközi összefogást és az interdiszciplináris elemzéseken alapuló cselekvést. Szintén mindkét jelenség sajátossága, hogy az európai társadalom és nyugati kultúrkörhöz tartozók szubjektív biztonságérzetét erősebben befolyásolják, mint a 2001-ben történt terrortámadás, illetve a 2015-ös tömeges irreguláris migrációt megelőző időszakban. Ennek egyik tényezője, hogy a két jelenség egyre nagyobb része lett a társadalmi és politikai közbeszédnek, amelyet a média nagyban alakít. A két jelenség közbeszédben betöltött szerepe miatt fontos, hogy állandó tudományos igényű és objektív elemzés tárgya legyen, hogy egy adott területegységhez tartozó társadalom működése hogyan alakítja és kezeli a migráció és a radikalizáció (amely a terrorizmushoz vezető út) társadalmi folyamatait.

Vizsgálataink szerint úgy tűnik, a menekülők nagy többsége nem azért jött Európába, hogy terrorcselekményeket kövessen el, hanem a Nyugat (az USA és szövetségesei) teremtett olyan helyzetet sok országban, hogy a terror eluralkodhatott, instabillá vált az adott állam működése, ezért kellett elmenekülnie sok millió embernek a szülőföldjéről, akiknek egy kis része az EU-ban számítana menedékre. Ezzel együtt talán bizakodóvá tehetnek minket azon adatok, amelyek globálisan, és főleg az EU-t is érintő irreguláris migránsok származási országaiban a terrorcselekmények csökkenő számát mutatják, és a schengeni térségbe érkező irreguláris migránsok száma[70] 2015-től folyamatosan csökken, ahogy a terrorcselekmények száma is.

---

[69] Osztrák Szövetségi Belügyminisztérium: A bécsi terrortámadást vizsgáló bizottság zárójelentése; https://www.bmi.gv.at/downloads/Endbericht.pdf (Letöltés ideje: 2022. 02. 23.)

[70] Frontex (European Border and Coast Guard Agency – Európai Határ- és Partőrség Ügynökség) adatok – forrás: http://frontex.europa.eu/publications – Letöltés ideje évente.

A tanulmány lezárását követően tört ki az orosz-ukrán háború, amely szintén jól illusztrálja, hogy a terror, a fegyveres konfliktus generálja igazán a menekülést, a migrációt.[71] Ezen események feldolgozása viszont már egy következő kutatás tárgya lehet.

Felhasznált irodalom:

- ALMADI Sejla: A bevándorlással kapcsolatos francia közvélemény 2012 és 2017 közötti alakulása; KKI-tanulmányok, a Külügyi és Külgazdasági Intézet időszaki kiadványa, T-2018/05.
- ANTAL Zsolt – GAZSÓ Tibor – KUBINYI Tamás – PELLE Veronika (Szerk.): Médiabefolyásolás – Az új kislexion. Századvég Kiadó, Budapest, 2015.
- BÁCS Zoltán György: A radikalizáció és a terrorizmus kapcsolata, egyes formái, gondolatok a megelőzés lehetséges perspektíváiról; Nemzetbiztonsági Szemle, Budapest, 2017/1. http://epa.oszk.hu/02500/02538/00017/pdf/EPA02538_nemzetbiztonsagi_szemle_2017_01_005-026.pdf (Letöltés ideje: 2022. 02. 23.)
- BAKÓCZI Antal: Megismerési akadályok a terrorizmus kutatásában; Belügyi Szemle, 2015/7-8. pp. 88-105.
- BEN-AMI, Slomo: Demagógok múltja és jövője; HVG, 2016. 08. 18.
- BIZEUL, Yves – RUDOLF, Dennis Bastian: Politikai viták a migráció és integráció körül: koncepciók és esettanulmányok; Springer Kiadó, Wiesbaden, 2019.
- BRECHER, Philippe – BEGASS, Christian – KRAFT, Josef: A mélység előretörése−AfD, Pegdida társai: a szalonoktól az utcáig; Pappy Rossa Kiadó, Köln, 2015.
- CSEPELI György: A kihűlt olvasztótégely; Belügyi Szemle, 1999/1. pp. 21-26.
- CSÍKSZENTMIHÁLYI Mihály: A fejlődés útjai. A harmadik évezred pszichológiája; Nyitott Könyvműhely, Budapest, 2007.
- CSUKA Gyöngyi – TÖRÖK Ádám (Szerk.): Az Európába irányuló és 2015-től felgyorsult migráció tényezői, irányai és kilátásai; MTA, Budapest, 2015.
- DEÁK József: A terrorizmus természete és az ellene történő fellépés nehézségei Oroszországban a Szovjetunió szétesésétől napjainkig; Belügyi Szemle, 2015/7-8. pp. 137-151.
- DEÁK József: Az Oroszországi Föderáció határőrizeti kihívásai napjainkban; Hadtudomány, 2016/E-szám, p. 7. URL.:http://mhtt.eu/hadtudomany/2016/2016_elektronikus/1_deak%20jozsef.pdf (Letöltés ideje: 2020.09.03.)

[71] Ez a legnagyobb humanitárius válság Európában a második világháború óta – mondta Jean-Christophe Dumont, az OECD migrációs kérdésekkel foglalkozó részlegének vezetője. Lásd: https://www.napi.hu/nemzetkozi-gazdasag/menekult-ukrajna-eu-europa-valsag-haboru-orosz.748654.html (Letöltés ideje: 2022. 03. 24.)

- DEÁK József: Határőrizeti és testületi modernizációtól a mai népvándorlás határrendészeti kezeléséig: a határrendészeti tisztképzés negyedszázada; Határrendészeti tanulmányok, 2017/2. pp. 70-79.
- Európa Biztonsági Stratégia; Az Európai Unió Kiadóhivatala, Luxembourg, 2009.
- European Commission Directorate-General Justice, Freedom and Security – SOLID/2007/27 – Committee General programme Solidarity and Management of Migration Flows meeting 20 September 2007.
- FÓRIZS Sándor: Menekültügyi válsághelyzet 1947-ben; Belügyi Szemle, 2015/2. pp. 149-163.
- FREUD, Sigmund: Mózes; Európa Kiadó, Budapest, 1987.
- GÖRBE Attiláné ZÁN Krisztina: „Mi" és „ők". Migráció és idegenellenesség a társadalmi megítélés tükrében; DOBÁK Imre (Szerk.): Szakmaiság, szerénység, szorgalom; Dialóg Campus Kiadó, Budapest, 2018. pp. 241-251. ISBN: 978-615-5889-51-6
- GÖRBE Attiláné ZÁN Krisztina: Nemzetközi xenofóbia kutatások; In: DEÁK József – GAÁL Gyula – SALLAI János (Szerk.): A toll sokszor erősebb, mint a kard: rendészettudományi tanulmányok Prof. Dr. Fórizs Sándor 65. születésnapja tiszteletére; 2016. pp. 84-100. ISBN: 9786155527982
- HAUTZINGER Zoltán: A terrorizmus elleni küzdelem idegenjogi eszközei; In: GAÁL Gyula − HAUTZINGER Zoltán (Szerk.): Pécsi Határőr Tudományos Közlemények, 2015. Pécs, pp. 203-212.
- HAUTZINGER Zoltán: Idegen a büntetőjogban; AndAnn Kft., Pécs, 2016.
- KESERŰ Dávid – GLIED Viktor: Migrációs tendenciák, kihívások és az erre adott szakpolitikai válaszok az Európai Unióban; In: TARRÓSY István – GLIED Viktor – VÖRÖS Zoltán (Szerk.): Migrációs tendenciák napjainkban; IDResearch Kft./Publikon Kiadó, Pécs, 2014.
- KOVÁCS Gábor: A migráció bűnügyi hatásai a magyar határrendészet kockázatelemzési rendszerére; In: HAUTZINGER Zoltán (Szerk.): A migráció bűnügyi hatásai; Magyar Rendészettudományi Társaság Migrációs Tagozat, Budapest, 2016. pp. 141-150.
- KOVÁCS Gábor: A rendőrség vezetésirányítási rendszerének sajátosságai a migrációs válsághelyzet kezelése során; In: TÁLAS Péter (Szerk.): Magyarország és a 2015-ös európai migrációs válság; Dialóg Campus Kiadó, Budapest, 2017. pp. 125-148.
- MASLOW, Abraham: Elmélet az emberi motivációról; Psychological Review, 1943/50. pp. 370-396.
- NAGY Gábor: Amerikai rémálom; HVG, 2016. 05. 26.
- PETHŐ-KISS Katalin: Countering Terrorist Act Against Christian Places of Worship; Perspectives on Terrorism, 2020 June/XIV. pp. 75-88.

- PÓCZIK Szilveszter: Az etnikai tényező és a halmozottan hátrányos helyzetű roma kisebbség kriminológiai nézőpontból; Kriminológiai és kriminalisztikai tanulmányok, Budapest, 1999, pp. 162-203.
- PÓCZIK Szilveszter: Nemzetközi migráció, biztonságpolitika, biztonság; In: TARRÓSY István – GLIED Viktor – VÖRÖS Zoltán (Szerk.): Migrációs tendenciák napjainkban; IDResearch Kft./Publikon Kiadó, Pécs, 2014.
- RITECZ György – SALLAI János: A migráció trendjei, okai és kezelésének lehetősége 2.0; Hanns Seidel Alapítvány, Budaörs, 2016.
- RITECZ György: A Migráció a XXI. század kezdetén; Globe Edit, Saarbrücken, 2017.
- RITECZ György: A tömeges migráció és/vagy népvándorlás ürügyén. A kialakult tömeges migráció katalizátorai; In: DEÁK József – GAÁL Gyula – SALLAI János (Szerk.): A toll sokszor erősebb, mint a kard; NKE Szolgáltató Kft., Budapest, 2016. pp. 174-189.
- RITECZ György: Az Európába irányuló tömeges irreguláris migráció felfutásának és megszűnésének okai. Hadtudomány, 2018/3-4. pp. 66-78.
- RITECZ György: Terrorizmus és/vagy bevándorlás avagy, mit mutatnak a számok; Migráció és Társadalom, 2015/1. pp. 112-120.
- ROSTOVÁNYI Zsolt: Iszlám, migráció, terrorizmus; http://ezredveg.vasaros.com/, 2016. (Letöltés ideje: 2022. 02. 27.)
- SIK Endre – TÓTH Judit (Szerk.): Migráció és politika; MTA Politikai Tudományok Intézet, Budapest, 1997.
- SIK Endre (Szerk.): A migráció szociológiája; Szociális és Családügyi Minisztérium, Budapest, 2001.
- SUHAJDA Attila: Politikailag motivált bűnözés és a migráció kapcsolata Németországban 2014 és 2020 között − kézirat
- SZABÓ A. Ferenc: A nemzetközi migráció és korunk biztonsági kihívásai; Zrínyi Kiadó, Budapest, 2006.
- TÁLAS Péter: A terrorfenyegetettségről a számok tükrében; Nemzet és Biztonság, 2011/7. pp. 83-92.
- TARRÓSY István – GLIED Viktor – VÖRÖS Zoltán (Szerk.): Migrációs tendenciák napjainkban; IDResearch Kft. – Publikon Kiadó, Pécs, 2014.
- TEKE András: A „pull–push factor" biztonság alapú megközelítése; Magyarországot érintő nemzetközi migráció – Felsőoktatási tankönyv. MK Katonai Biztonsági Hivatal, Budapest, 2006.
- TÓTH Pál Péter: Nemzetközi vándormozgalom; Belügyi Szemle, 1999/1. pp. 27-34.

Statisztikák:

- 25 Years of global forced displacement. www.unhcr.org/statistics (Letöltés ideje: 2015. 02. 05.)
- EUROPOL TE-SAT European Union Terrorism situation and trend report 2008 és 2021 közötti kiadványai. www.europol.europa.eu (Letöltés ideje: évente)
- GTD. www.start.umd.edu/data-tools/global-terrorism-database-gtd (Letöltés ideje: 2010 és 2021. között évente)
- UNHCR Global Trends Forced Displacement 1993 és 2021 éves kiadványai. www.unhcr.org (Letöltés ideje: 2002 és 2022. között évente.)

Internetes források:

- http://solidalapok.hu (Letöltés ideje: 2015. 01. 23.)
- http://hvg.hu/hvgfriss/2015.03/201503_muszlimok_dzsihadistak_es_rasszistak_europa (Letöltés ideje: 2015. 04. 02.)
- http://navyseals.hu/tortenelem/szomalia/a_mogadishui_csata.html (Letöltés ideje: 2015. 07. 18.)
- Szövetségi Alkotmányvédelmi Hivatal kompendiuma: az egyes szakterületek és megfigyelési objektumok bemutatása. Szövetségi Alkotmányvédelmi Hivatal, Köln, 2018. pp. 1-119. https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/allgemein/2018-12-kompendium-des-bfv-darstellung-ausgewaehlter-arbeitsbereiche-und-beobachtungsobjekte.html (Letöltés ideje: 2022. 02. 23.)
- Szövetségi Alkotmányvédelmi Hivatal: Helyzetjelentés − jobboldaliak a rendészeti szerveknél. Köln, Szövetségi Alkotmányvédelmi Hivatal, 2020. https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/rechtsextremismus/2020-09-lagebericht-rechtsextremisten-in-sicherheitsbehoerden.html (Letöltés ideje: 2022. 02. 23.)
- Szövetségi Bűnügyi Hivatal: Politikailag motivált bűncselekmények – szövetségi adatok. Wiesbaden, 2021. p. 3. https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/210504_PMK2020.html (Letöltés ideje: 2022. 02. 25.)

TÓTH TAMÁS

MAGYARORSZÁG NEMZETI BIZTONSÁGI STRATÉGIAI EVOLÚCIÓJA, ANNAK AKTUALITÁSAI ÉS FŐBB NEMZETBIZTONSÁGI VETÜLETEI

Bevezetés

A 21. század biztonsági környezetét elemezve megállapítható, hogy korunkra számos kihívással, kockázattal és fenyegetéssel kell szembenéznünk. Napjainkban mind a globális, mind a regionális, mind a nemzeti biztonsági környezet dinamikus változáson megy keresztül. Számos, a biztonságot befolyásoló tényező azonosítható a kérdéskör vizsgálata során. Ahhoz, hogy ezekre az egyes államok és a szövetségesi rendszerek megfelelő prognosztikus szemléletű válaszokat tudjanak adni, szükséges a biztonsági környezet rövid, közép és hosszú távú elemzése. Az elemzés során levonható következtetések alapján kell meghatározni az egyes veszélyeztető tényezők körét, a védendő érdekeket, a célokat, valamint a célok eléréséhez szükséges intézkedések irányait, és az intézkedések megtételéért felelős szervezetek és eszközrendszerek körét, amelyeket az egyes állami és nemzetközi szereplők biztonsági tárgykörű stratégiai dokumentumokban deklarálnak.[1] A „stratégia" alapvetően a jövőbeli célokról, víziókról és a beteljesüléséhez szükséges átfogó intézkedésekről szól, amely eléréséhez sajátos tervezési módszerek alakultak ki.[2]

Sabjanics István kutatási eredményei szerint a (nemzet)biztonsági stratégiának, „*mint minden kormánypolitikát, nemzetpolitikát és állami stratégiai irányokat tartalmazó dokumentumnak egyértelműen politikai tartalma és üzenete van abban az értelemben, hogy értékválasztás alapján a társadalmi életviszonyokat befolyásolja.*"[3] Csiki Tamás 2014-ben publikált kutatási eredményei szerint „*Kelet-Közép-Európa országainak az elmúlt 25 évben háromszor kellett mélyrehatóan átalakítaniuk védelempolitikájukat: a hidegháborús szembenállás végére, az euroatlanti integráció sikerére, valamint a 2008-as gazdasági válság mélyreható következményeire reagálva."*[4] 2014-et követően védelmi, biztonsági stratégiaalakító hatásuk okán globális vetületen kiemelendő a kibertér és a hibrid hadviselés/bűnözés befolyásoló szerepe, 2020-tól a SARS-CoV-2 világjárvány, perspektivikusan pedig a világűr központi potenciálja a biztonság területén. Regionális, európai szinten is tapasztalhatóak voltak jelentős események, kiemelten a 2015-től fokozódó tömeges illegális migrációs válság, az iszlám fundamentalista terrorizmus térnyerése, valamint legaktuálisabban a 2022-es ukrán-orosz fegyveres konfliktus szintén védelmi

[1] DOBÁK Imre – TÓTH Tamás: A külső környezet, és tendenciák nyomon követésének szükségessége a stratégiaalkotás tükrében. In: (szerk): Stratégiák, stratégiai gondolkodás, nemzetbiztonság, TKP2020-NKA-09., Budapest, Ludovika Egyetemi Kiadó, 2022. (Megjelenés alatt.)

[2] FITZSIMMONS, Michael: Scenario Planning And Strategy In The Pentagon; Strategic Studies Institute US Army War College, Pennsylvania, 2019. p. 24. ISBN 158-487-801-1

[3] SABJANICS István: A nemzetbiztonság jogi koncepciója, In: CSINK Lóránt (Szerk.): A nemzetbiztonság kihívásainak hatása a magánszférára, Budapest, 2017, Pázmány Press. p. 114. ISBN 978-963-308-319-2

[4] CSIKI Tamás: Az új Nemzeti Katonai Stratégia a nemzetközi tapasztalatok tükrében; Nemzet és Biztonság, 2014/2. p. 45. ISSN 1789-5286

stratégiaalakító hatást gyakorol a térségre, amelyek normatív leképeződése aktuális folyamat.

Magyarország a jogállamiság 1989. október 23-ai restitúcióját követő évtizedben szerzett érvényt a védelmi stratégiaalkotás normatív gyakorlatának, amely keretében alapelveket fogalmazott meg mind a biztonságpolitika, mind a honvédelem vetületén. Az alapelvekre épített stratégiákat a 21. század újabb és újabb biztonságot befolyásoló tényezőinek figyelembevételével tartalmilag, formailag azóta is aktualizálja a jogalkotó hiszen „*A biztonság szavatolása alapvető nemzeti érdekünk és az alaptörvényben rögzített feladatunk*."[5] A 2020. április 22-től hatályos Magyarország Nemzeti Biztonsági Stratégiájának[6] 126. pontja alapján *„Magyarország stratégiai célkitűzése, hogy 2030-ra kialakítsa azokat a nemzeti ellenálló, elrettentési, védelmi, válságkezelési és koordinációs képességeket, amelyek a változékony nemzetközi környezetben előfeltételei a nemzet fejlődéséhez szükséges stabilitásnak és biztonságnak. Magyarország nemzetközi összehasonlításban is magas szintű közbiztonsági helyzetét meg kell őrizni és tovább kell javítani."* A fenti stratégiai célkitűzések megvalósítása elképzelhetetlen lenne a megfelelő politikai és szakmai döntések meghozatalához szükséges releváns információk megszerzését, feldolgozását, elemzését-értékelését végző hazai nemzetbiztonsági szolgálatok nélkül, amelyek szerepe egyre fokozottabban felértékelődik.

Jelen publikáció fő célja a hazai biztonsági és védelmi tárgyú alapelvek, valamint az átfogó biztonsági stratégiáik evolúciójának áttekintése, kiemelve azok nemzetbiztonsággal kapcsolatos főbb rendelkezéseit, behatóbban elemezve azokat a hatályos 2020-as Nemzeti Biztonsági Stratégia kapcsán. Továbbá a tanulmány a nemzeti biztonság stratégiai vetületén megjelenő aktualitásokat, a közelmúltban végbement főbb jogalkotási irányokat kívánja részletesebben áttekinteni a nemzetbiztonsági szolgálatok kormányzati irányításával összefüggő, 2022. május 25-ig megjelenő jogszabályi változásokig[7] bezárólag, alátámasztva a nemzetbiztonsági ágazat fokozódó szerepét a biztonsági stratégiai célok megvalósítása terén.

Magyarország nemzeti biztonságának átfogó stratégiai evolúciója

Hazánk nemzeti biztonságának stratégiai szintű fejlődése a jogállamiság 1989. október 23-ai helyreállítását, valamint a Varsói Szerződés 1991. július 01-jei felbomlását követő transzatlanti orientációjú demokratikus időszak vonatkozásában kerül elemzésre, egészen napjainkig. A biztonsági, védelmi tárgykörű korábbi

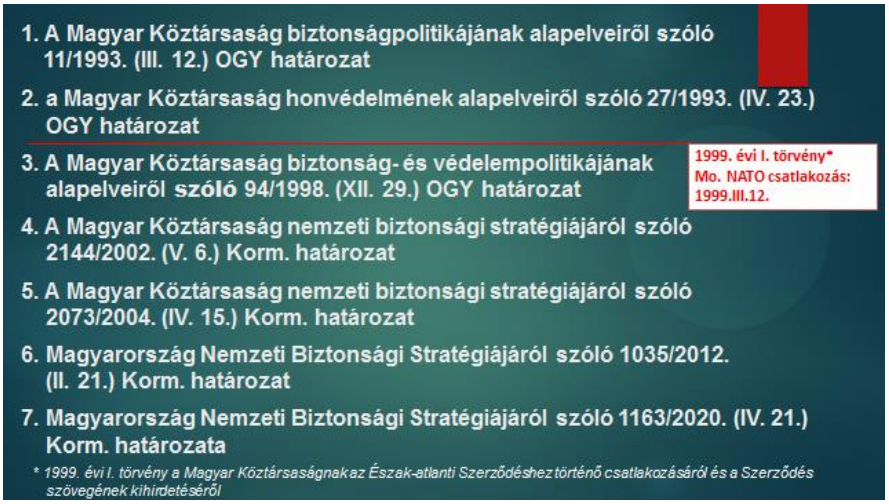
---

5 KUN SZABÓ István vezérőrnagy – SANDRA Sándor ny. o. ezredes – STICZ László ezredes: Haza, biztonság, honvédelem, haderőfejlesztés; Honvédségi Szemle, 2018/5. p. 141. ISSN 2060-1506

6 1163/2020. (IV. 21.) Korm. határozat 1. sz. melléklete

7 Tekintettel arra, hogy a tanulmányban később vizsgált jogszabályok (pld. Nbtv.; Vbö; Statútum rendelet stb.) által előirányzott változások végrehajtásához egy sor alacsonyabb jogforrás is tartozik, amelyek még javaslat szinten is csak korlátozottan kerültek megfogalmazásra, ezért jelen publikáció a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény legutóbbi 2022. május 25-én hatálybalépett módosítását, és az azt megelőző időszakot dolgozza fel.

stratégiák mélyebb tartalmi szempontú elemzését számos szerző feldolgozta[8], ezért evolúciójukat elsődlegesen „identitási" és jogalkotási oldalról kívánom vizsgálni, kiemelve azok nemzetbiztonsági szempontú rendelkezéseit, részletezve azokat a hatályos 2020-as stratégia kapcsán. Kezdő lépésként az alábbi, 1. ábrán kerül szemléltetésre Magyarország biztonsági tárgykörű stratégiáinak átfogó evolúciós fejlődése, amelybe jelen tanulmány vonatkozásában beleértendőek az egyes biztonsági és védelmi tárgyú alapelveket deklarálni hivatott tervdokumentumok[9] is.



1. ábra: Hazai nemzeti biztonsági átfogó stratégiák fejlődése
(saját szerkesztés)

Az 1990-es évektől a Kelet-közép-európai térségben egyfajta biztonság-, gazdaság- és társadalompolitikai irányváltás volt megfigyelhető, amely a Szovjetunió felbomlásával, a kétpólusú világrend megszűnésével, valamint a volt szovjet befolyási övezet „demokratizálódásával" új geopolitikai helyzetet teremtett, amely az államok átfogó stratégiai céljaiban is testet öltött. Tálas Péter elemzése szerint „*a gazdasági-társadalmi válságból való kilábalás és a gyors modernizáció reményében ugyanis a bipoláris világrend összeomlását követően szinte valamennyi kelet-közép-európai nemzet céljai között megjelent az európai politikai értékeken alapuló demokratikus jogállam és a piacgazdaság kialakítása, az európai gazdasági, illetve az euroatlanti biztonsági szervezetekhez való közeledés szándéka, s ezzel együtt a szuverenitás-megosztás tudatos felvállalása. Másfelől viszont – a tömbpolitika által évtizedekig rájuk oktrojált korlátozott szuverenitás fogságából kiszabadulva – valamennyien*

[8] Pld. KISS Petra: A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében; Hadtudomány, 2012/3-4. pp. 68-79. ISBN: 978-963-531-615-1; TEKE András: A rendészet/rendvédelem tartalmi és funkcionális megjelenítése a magyar (nemzeti) biztonsági stratégiákban/stratégiai dokumentumokban (1993-2020); Határrendészeti tanulmányok, 2021/3. pp. 84-132. ISSN 2061-3997

[9] Ezen alapelveket magukba foglaló tervdokumentumok célja, hogy meghatározzák a kormány és a további illetékes szereplők számára, hogy mely fő elvek, irányok és célok szerint tervezze és hajtsa végre az ország védelmi és biztonsági célú felkészítését, illetve képességeinek fejlesztését, fenntartását és működtetését. (Forrás: A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény 22. § (3))

újrafogalmazták nemzeti érdekeiket, önálló kül- és biztonságpolitikájukat, s igyekeztek az adott körülmények között a lehető legteljesebb körűvé tenni szuverenitásukat (szuverenitás-kiteljesítés).”[10] Ezen igény természetesen a magyar törvényhozás számára is megfogalmazódott, amelynek eredményeképpen az 1. ábrán is szemléltetve elfogadásra került a Magyar Köztársaság biztonságpolitikájának alapelveiről szóló 22/1993. (III.12.) OGY határozat, valamint a Magyar Köztársaság honvédelmének alapelveiről szóló 27/1993. (IV.23.) OGY határozat, még szekularizáltan kezelve a biztonságpolitika és honvédelem, védelempolitika „stratégiai” kérdéskörét. A magyar biztonság- és védelempolitikai alapelvek 1993-as külön dokumentumokban történő elfogadását követő öt évben mind a globális geopolitikai helyzet, mind az euroatlanti viszonyrendszer, mind pedig Magyarország regionális környezete változásokon ment keresztül. *„A délszláv válság 1991-től 1995-ig tartó időszaka lezárult ugyan a daytoni egyezmények aláírásával, ám Koszovó helyzete egyre kritikusabbá vált. Magyarország, a magyar biztonságpolitika szempontjából kiemelkedő fontosságú volt a közelgő NATO-csatlakozás és az abból adódó új biztonságpolitikai helyzet. Ez szükségessé tette a korábbi biztonságpolitikai alapelvek felülvizsgálatát, újak létrehozását.*”[11]

A biztonsági és védelmi tárgyú alapelvek, tervdokumentumok kapcsán a következő tényleges evolúciós lépést Magyarország 1999. március 12-ei NATO-[12] csatlakozása[13] hozta el. Az 1. ábrán a piros vonal nem tévesztésből szerepel az 1998-ban kiadott újabb hosszútávra vonatkozó, elvi szintű védelmi és biztonsági tervdokumentumot megelőzően, hanem fejlődési szakaszt hivatott szemléltetni. Ennek magyarázata a NATO-csatlakozást szabályozni hivatott, a Magyar Köztársaságnak az Észak-atlanti Szerződéshez történő csatlakozásáról és a Szerződés szövegének kihirdetéséről szóló 1999. évi I. törvény 2. §-nak, valamint a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről szóló 94/1998. (XII. 29.) OGY határozat hatálybalépésének szoros összefüggése. A 94/1998 (XII. 29.) OGY határozat már prognosztikus szemléletben a NATO-csatlakozás által hazánk számára várható új biztonsági környezetnek megfelelően került kidolgozásra, amelyre mi sem kifejezőbb elköteleződés a határozat 3. pontjánál. E szerint *„ez a határozat a Magyar Köztársaságnak az Észak-atlanti Szerződéshez történő csatlakozásáról és a Szerződés szövegének kihirdetéséről szóló törvény 2. §-a hatálybalépésének napján lép hatályba. Ezzel egyidejűleg hatályát veszti a Magyar Köztársaság biztonságpolitikájának alapelveiről szóló 11/1993. (III. 12.) OGY határozat, és a Magyar Köztársaság honvédelmének alapelveiről szóló 27/1993. (IV. 23.) OGY határozat*.” Tehát a felülvizsgált, 1998-as alapelveket tartalmazó dokumentum *pro futuro*, a törvény 2. §-nak 1999. június 21-ei hatálybalépésével vált hatályossá, azonban a törvény 2 §-nak rendelkezései Magyarország 1999. március 12-ei NATO-

---

[10] TÁLAS Péter: A nemzeti katonai stratégia és a magyar stratégiai kultúra; Hadtudomány, 2013/3-4. pp. 22-23. ISBN: 978-963-531-615-1

[11] IGNÁTH Éva: Az Országgyűlés 94/1998. (XII. 29.) sz. határozata a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről; Grotius, 2009. p. 1.

[12] North Atlantic Treaty Organisation – Észak-atlanti Szerződés Szervezete

[13] Kihirdetve: A külügyminisztertől Közlemény a Washingtonban, 1949. április 4-én létrehozott Észak-atlanti Szerződésnek a Magyar Köztársaság vonatkozásában történt hatálybalépéséről, 1999. 03. 26. Magyar Közlöny, 1990/25. p. 1760.

csatlakozásától alkalmazandók[14]. Ezen jog- és tervdokumentum-alkotási metódus egyben a NATO csatlakozáshoz fűződő atlantista szemléletű stratégiai lépésként értékelhető, amely már integráltan kívánta kezelni és szabályozni a biztonsági és védelempolitikai alapelveket, előzetesen illeszkedve a NATO új 1999. évi Stratégiai Koncepciójának[15] szellemiségéhez, például a biztonság átfogó értelmezésének területén. „*A biztonságot e szerint átfogó módon kell értelmezni, amely a politikai és katonai tényezőkön túl magában foglalja a gazdasági és pénzügyi, emberi jogi és kisebbségi, információs és technológiai, környezeti, valamint nemzetközi jogi biztonságot is, amely az euroatlanti térségben a kölcsönös függőség miatt oszthatatlan*."[16]

A biztonsági stratégiaalkotással kapcsolatos első érdemi evolúciós lépés az Országgyűlés által 1998-ban elfogadott biztonság- és védelempolitikai alapelvekkel összhangban a Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2144/2002. (V. 6.) Korm. határozattal hatályba léptetett stratégiai tervezési dokumentum, mely egyben Magyarország első átfogó nemzeti biztonsági stratégiája. Preambuluma szerint „*Az alapelvekre, valamint a NATO 1999-ben elfogadott Stratégiai Koncepciójára épül a Magyar Köztársaság nemzeti biztonsági stratégiája, amelynek rendeltetése, hogy a nemzeti értékek és érdekek, valamint a nemzetközi környezet és adottságok alapján megfogalmazza az országot érő biztonságpolitikai kihívásokat, illetve mindezek alapján meghatározza a magyar biztonságpolitika stratégiai feladatait.*" Jelen tanulmány szempontjából kiemelendő, hogy a 2002-es stratégiában a célkitűzések megvalósítása érdekében már megjelent a nemzetbiztonsági szolgálatok[17] szerepe például a szervezett bűnözés, a terrorizmus, az illegális migráció, valamint belső társadalmi átalakuláshoz köthető negatív jelenségek megelőzése és kezelése kapcsán.

2004-ben a 2073/2004. (III. 31.) Korm. határozattal kiadásra került a soron következő új nemzeti biztonsági stratégia, amely már magában hordozta Magyarország 2003. április 12-ei európai uniós csatlakozásból fakadó értékeket is. A 2004-es stratégia preambuluma értelmében „*a Magyar Köztársaság biztonság- és védelempolitikájának alapelveire épít, és összhangban van a NATO 1999. évi Stratégiai Koncepciójával és az EU által 2003-ban elfogadott Európai Biztonsági Stratégiával*."[18] A 2004-es stratégiában a korábbihoz képest hangsúlyosabb a nemzetbiztonsági szolgálatok szerepe a kormányzati döntés-előkészítés, az ország szuverenitásának, alkotmányos rendjének védelme és nemzetbiztonsági érdekeinek érvényesítése terén, valamint nyomatékosításra kerül az ágazaton kívüli

---

[14] 1999. évi LVIII. törvény a Magyar Köztársaságnak az Észak-atlanti Szerződéshez történő csatlakozásáról és a Szerződés szövegének kihirdetéséről szóló 1999. évi I. törvény módosításáról 3. §

[15] The Alliance's Strategic Concept; 1999. április 24. Press Release NAC-S(99) p. 65.

[16] DR. ALMÁSI Ferenc alezredes: Honvédelmünk NATO integrációs folyamatának áttekintése, tapasztalatai és következtetései jogi szempontból; Doktori (PhD) értekezés, ZMNE HDI, Budapest, 2005. p. 34.

[17] Ekkor már a nemzetbiztonsági szolgálatok tevékenységét és a szervezetrendszer felépítését az 1996. március 27-én hatályba lépett nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény szabályozza, amely értelmében nemzetbiztonsági szolgálat volt az Információs Hivatal, a Nemzetbiztonsági Hivatal, a Nemzetbiztonsági Szakszolgálat, a Katonai Felderítő Hivatal és a Katonai Biztonsági Hivatal.

[18] 2073/2004. (III. 31.) Korm. határozat 1. sz. melléklet preambuluma

együttműködés jelentősége is. A 2004-es stratégia kimondja, hogy a „*nemzetbiztonsági szolgálatoknak a veszélyforrások felderítése és felszámolása céljából elhárító és hírszerző tevékenységet kell folytatniuk*".

Következő evolúciós lépésként 2012-ben elfogadásra került a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat. A 2004-es stratégiát követően, mintegy 8 év telt el annak felülvizsgálatáig, amelyet többek között a megelőző időszak során bekövetkezett biztonsági környezeti és politikai változások, valamint Magyarország Alaptörvényének 2011. április 25-ei hatálybalépése és az által meghatározott biztonsági garanciális célok is indukáltak. Kiss Petra szerint a 2012-es stratégiát „*összehasonlítva a 2002-ben, illetve 2004-ben elfogadott stratégiákkal, egyértelműen egy nyugati, azon belül is az Egyesült Államok stratégiaalkotásához közelítő tendenciát figyelhetünk meg a dokumentum szerkezetében és tartalmában.*"[19] A stratégia tovább mélyíti a biztonság átfogó értelmezésének vetületét, amely 2. pontja szerint „*egyre inkább előtérbe kerülnek azok a biztonságpolitikai kihívások, amelyek kezeléséhez átfogó és összehangolt politikai, gazdasági és – szükség esetén – katonai fellépésre van szükség*". A 2012-es stratégia a haderőfejlesztés kapcsán is kiemelendő, hiszen a kormány ez alapján ágazati stratégiaként megalkotta például a 2012-es Magyarország Nemzeti Katonai Stratégiáját,[20] amely végrehajtásához kapcsolódóan 2017-ben kihirdetésre került a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program.[21] A 2012-es stratégia 31. pontjában a Magyarországot érintő biztonsági fenyegetések és kihívások kapcsán új tényezőként megjelent a kiberbiztonság és annak garantálása érdekében a nemzetbiztonsági ágazat szerepe is, amely fokozódó hangsúlyosságát a kormány által 2013. március 23-án elfogadott és hatályos Magyarország Nemzeti Kiberbiztonsági (ágazati) Stratégiája[22] is jelez. A 2012-es stratégia továbbmélyíti a nemzetbiztonsági szolgálatok együttműködésének igényét a honvédelmi, rendvédelmi, igazságügyi és polgári védelmi szervekkel. Megemlítendő, hogy a nemzetbiztonsági szervezetrendszerben is jelentős változás következett be 2012-ben. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) 2011. novemberi módosítása, valamint a 128/2011. (XII. 2.) HM utasítás alapján 2011 decemberében megkezdődött a katonai elhárítási tevékenységi körrel rendelkező Katonai Biztonsági Hivatal és a katonai hírszerzésért felelős Katonai Felderítő Hivatal integrációjának előkészítése, mely eredményeképpen 2012. január 01-jén a két katonai szervezet összevonásával megalakult a Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ).[23]

---

19 KISS i. m. p. 60.

20 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról

21 Itt megjegyzendő, hogy a korábbi átfogó nemzeti biztonsági stratégiák is előírták egyes biztonsági tárgykörű ágazati stratégiák megalkotását, azonban ezek csak korlátozottan kerültek megvalósításra.

22 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

23 KENEDLI Tamás: A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években; Nemzetbiztonsági Szemle, 2020/1. pp. 77-78. ISSN 2064-3756

Többek között Európát 2015-től fokozottan érintő migrációs válság, az iszlám fundamentalista terrorizmus térnyerése, az új és innovatív technológiák által megjelenő globális hibridjellegű biztonsági kihívások, a kiberbiztonságot veszélyeztető tevékenységek fokozódása, valamint a világűrben rejlő lehetőségek biztonsági célú kiaknázhatósága átfogó biztonsági stratégiai felülvizsgálatra késztette a kormányt. 2016. november 24-én a honvédelmi, a Miniszterelnökséget vezető miniszter, a belügyminiszter, illetve a külgazdasági és külügyi tárca vezetőjének a Nemzeti Biztonsági Stratégia felülvizsgálatára létrehozott munkacsoportról szóló 57/2016. (XI. 24.) HM-MvM-BM-KKM együttes utasítása alapján a 2012-es nemzeti biztonsági stratégia felülvizsgálatára tárcaközi munkacsoportot hoztak létre, amelynek vezetője a Honvédelmi Minisztérium védelempolitikáért és védelmi tervezésért felelős helyettes államtitkára lett. E munkacsoport tevékenysége nyomán 2020. április 23-án hatályba lépett a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat, és egyben annak 1. számú mellékleteként a „*Biztonságos Magyarország egy változékony világban”* című átfogó nemzeti biztonsági stratégia (a továbbiakban: Stratégia).

A Stratégia világképe Csiki Varga Tamás és Tálas Péter elemzése szerint „*reálpolitikai, és a globális biztonsági helyzet romló tendenciájával, biztonsági környezetünk jellemzőinek fokozatos romlásával számol a 2020-as évtizedben. Ugyanakkor azonosítja azokat a lehetőségeket is, amelyek elősegíthetik érdekeink érvényesítését*.”[24] A Stratégia fő célja az ország jelenlegi biztonsági szintjének megőrzése és erősítése, valamint az ország további fejlődésének biztosítása, továbbá Magyarország stratégiai célkitűzése, hogy 2030-ra kialakítsa azokat a nemzeti ellenálló, elrettentési, védelmi, válságkezelési és koordinációs képességeket, amelyek előfeltételei a nemzet fejlődéséhez szükséges stabilitásnak és biztonságnak. Ennek érdekében a Stratégia kiemeli többek között a nemzetbiztonsági szolgálatok fokozott szerepét, hiszen a Stratégia 126. pontja alapján a „*biztonság elsődleges alapja a szilárd társadalmi, gazdasági és pénzügyi szerkezet, valamint nemzeti szinten a megelőző és védelmi intézkedések fenntartható és rugalmas rendszere, ezen belül pedig a haderő, valamint a rendvédelmi szervek ([…] a nemzetbiztonsági szolgálatok, […]) célirányos fejlesztése.*” A Stratégia a hazai védelmi ipar fejlesztésének támogatását is nemzetbiztonsági érdekként határozza meg, akárcsak az innováción alapuló űrszektor nemzetbiztonsági célú hozzáférését. Továbbra is cél a korábbi stratégiákban szintén megjelenő szervezett bűnözés, terrorizmus, illegális migráció megelőzésében és felderítésében való részvétel. Új elemként került beemelésre a hibrid támadások leleplezésében és elhárításában való közreműködés, illetve a Stratégia tovább mélyíti a nemzetbiztonsági szolgálatok ágazatokon átívelő együttműködésének igényét nemzeti és nemzetközi szinten egyaránt. A Stratégia 166. pontja *expressis verbis* a nemzetbiztonsági szolgálatok alapvető feladataként definiálja, hogy „*különleges műveleti eszközeik és módszereik hatékony felhasználásával derítsék fel és akadályozzák meg a Magyarország nemzeti érdekeit leplezett formában veszélyeztető törekvéseket, illetve azonosítsák a törekvések hátterében álló állami, illetve nem kormányzati szereplőket*.” A biztonsági környezet romlása okán szükségesnek tartja a nemzetbiztonsági szolgálatok képességeinek továbbfejlesztését, különös tekintettel a titkos információgyűjtés koncentrált eszközrendszerére.

---

[24] CSIKI VARGA Tamás – TÁLAS Péter: Magyarország új nemzeti biztonsági stratégiájáról; Nemzet és Biztonság, 2020/3. p. 111. ISSN 1789-5286

A Stratégia kiemelt kockázatként azonosítja a kormányzati és létfontosságú rendszereket veszélyeztető, érintő kibertámadásokat, -incidenseket. A kibervédelmi feladatok ellátása, a kiberbiztonság garantálása mellett központi célkitűzésként jelenik meg benne az offenzív kiberképesség kialakítása is. Ennek kapcsán az Nbtv. 2020. július 01-jei módosításának következtében egyrészről meghatározásra kerültek *„a kiber-védekezőképesség növelése érdekében végrehajtandó feladatok, másrészt az Nbtv. 56. § e) pontjának kiegészítésével lehetőség nyílt arra, hogy a nemzetbiztonsági szolgálatok a feladataik ellátásával összefüggésben a kibertérben észlelt fenyegetésekkel szembeni ellenintézkedésekre külső engedélyhez kötött titkos információgyűjtés keretében jogosultak legyenek.*”[25] A Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 191. § értelmében a 2022. május 25-ei hatállyal létrejött Védelmi Tanács[26] elnöke a 21. század kibertérből érkező fenyegetéseire adandó stratégiai válaszok mentén *„ügydöntő jogkörrel gyakorolja a Kormány részére a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 8. § (8) bekezdésében, valamint a honvédelemről és a rendkívüli intézkedésekről szóló 2011. évi CXIII. törvény 62/A. § (6a) bekezdésében meghatározott hatáskört.*” Azaz a miniszterelnök[27] döntési jogkörrel rendelkezik a Nemzetbiztonsági Szakszolgálat információbiztonsággal kapcsolatos feladatkörében a kibertérből érkező támadás megszakításához szükséges intézkedések, valamint a Magyar Honvédség katonai kibertér műveleteinek végrehajtása kapcsán.

A Stratégia 2. pontja értelmében 2021. december 31-ig annak ágazati leképeződése, végrehajtása érdekében elkészült például az aktualizált 2021-es Nemzeti Katonai Stratégia[28], azonban többek között a nemzetbiztonsági ágazati stratégia továbbra sem került kidolgozásra, amely feladat egyre aktuálisabbá válik.

A logikai gondolatmenetbe ékelve érdemes következtetéseket levonni a hosszú távú biztonsági- és védelempolitikai alapelveket meghatározó tervdokumentumok, valamint az ezekkel összefüggésben megalkotott átfogó biztonsági stratégiai tervezési dokumentumok anyagi jogi forrásának és a jogalkotó szerv jogkörének eredete kapcsán. Az alábbi 2. ábra alapján meghatározhatóak további következtetések, többek között az egyes alapelvek és stratégiák időbeli hatályának vonatkozásában, valamint azok elfogadásakor mandátummal rendelkező kormányok politikai összetétele tekintetében is, hiszen a biztonsággal kapcsolatos kihívások, kockázatok és fenyegetések mellett stratégiaalakító hatással bírnak az aktuális kormányzat politikai célkitűzései a főbb stratégiai prioritások meghatározásán keresztül.

---

[25] BARNÓCZKI László – KENEDLI-TÓTH Eszter: A nemzetbiztonsági szolgálatok megszervezése és működése az eltelt harminc év során – változások az ágazatot érő legfontosabb kihívások tükrében; In: CHRISTIÁN László – LIPPAI Zsolt – NÉMETH Zsolt (Szerk.): A rendszerváltás hatása a rendészetre; Ludovika Egyetemi Kiadó, Budapest, 2021. pp. 91-92. ISBN 978-963-531-554-3

[26] A 1144/2010. (VII. 7.) Korm. határozat 2022. május 25-ei módosításának hatálybalépésével a Védelmi Tanács kibővítve átvette a Nemzetbiztonsági Kabinet feladatkörét, annak egyidejű megszüntetésével.

[27] 1144/2010. (VII. 7.) Korm. határozat 90/D § (2) bek.

[28] 1393/2021 (VI. 24) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról

Kibocsájtás dátuma /hatályosság/	Jogforrás típusa (anyagi és alaki)	Jogalkotó szerv típusa (jogkör eredete szerint)	Kormányzó pártok
11/**1993** (III.12.) /1993.03.12 - 1999.06. 21/	OGY. határozat	elsődleges	MDF-FKGP-KDNP (Antal-kormány)
27/**1993** (IV. 23.) /1993.04.23 - 1999.06. 21/	OGY. határozat	elsődleges	MDF-FKGP-KDNP (Antal-kormány)
94/**1998** (XII.29.) /1999.06.21 – /	OGY. határozat	elsődleges	FIDESZ-FKGP-MDF (I. Orbán-kormány)
2144/**2002** (V.6.) /2002.05.07 -2005.09.01/	Korm. határozat	származékos	FIDESZ-FKGP-MDF (I. Orbán-kormány)
2073/**2004** (IV.15.) /2005.09.01 - 2012.02.22/	Korm. határozat	származékos	MSZP-SZDSZ (Medgyessy-kormány)
1035/**2012** (II.21) /2012.02.23 - 2020.04.22/	Korm. határozat	származékos	FIDESZ-KDNP (II. Orbán-kormány)
1163/**2020** (IV.21.) /2020.04.22- /	Korm. határozat	származékos	FIDESZ-KDNP (IV. Orbán-kormány)

2. ábra: Nemzeti biztonsági átfogó stratégiák összehasonlítása kibocsájtó szerint
(saját szerkesztés)

A 2. ábra alapján látható, hogy míg az 1993-as és 1998-as alapelveket az Országgyűlés eredeti, primer jogalkotói hatáskörében fogadta el, addig 2002-től a hatályos stratégiák a kormány szekunder, származékos jogalkotói jogkörében kerülnek elfogadásra. A stratégiai célok szakpolitikai ideológia mentén történő alakítása általános tendenciaként határozható meg. A hatályos Stratéga a kibocsátó vonatkozásában azért tér el a korábbi stratégiáktól, mert a kormányzó pártok összetétele nem változott az azt megelőző 2012-es stratégiához[29] képest, azt a második Orbán-kormány fogadta el, míg a 2020-ast a negyedik. A 2012-ben meghatározott stratégiai célok újragondolását a célkitűzések megvalósításán, a biztonsági környezet romló tendenciáján, az új kihívások és lehetőségek megjelenésén túl az is indukálhatta, hogy a kormány az első és második ciklust követően a harmadik 2018-2022. ciklusra olyan stabil belpolitikai, gazdasági környezetet teremtett, mely alapjául szolgálhatott a közép és hosszú távú, innovációra épülő gazdasági, technológiai és társadalmi fejlődésnek.[30] Ezen fejlődési tendencia Magyarország számára abban az esetben lesz fenntartható, ha továbbra is garantálásra kerül a komplex biztonság érvényesülése, mely érdekében szükséges a stratégiai célok és a végrehajtási intézkedések folyamatos aktualizálása, valamint a szükséges erőforrások rendelkezésre bocsátása.

Aktualitásirányok a nemzeti biztonság stratégiai vetületén

A 2021-2025. időszakot vizsgáló középtávú, 2021. decemberi Makrogazdasági és Költségvetési Előrejelzés[31] szerint 2021-ben a gazdasági növekedés beváltotta a korábbi éves pozitív előrejelzést, amely tendencia várhatóan 2022-ben is folytatódni fog, azonban a következő időszakban a SARS-CoV-2 világjárvány hosszú távú hatásaként lassuló növekedést prognosztizál a főbb gazdasági centrumokban. Az

[29] 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról
[30] https://eacea.ec.europa.eu/national-policies/eurydice/content/political-and-economic-situation-35_hu (Letöltés ideje: 2022. 05. 01.)
[31] Makrogazdasági és Költségvetési Előrejelzés (2021-2025); Pénzügyminisztérium, Budapest, 2021. december

elemzés szerint a „*kedvezően alakuló belső kereslettel szemben azonban a növekedési előrejelzést számos lefelé mutató külső kockázati tényező övezi.*”[32] Ilyen kockázati tényező például a termelői és szállítási kapacitások szűkössége, a transznacionális ellátási láncok akadozása, a globális szinten felgyorsuló infláció, vagy például a megnövekedett energia- és alapanyagárak beépülése a feldolgozóipari termékek és szolgáltatások árába. Ezen, többségében gazdasági jellegű kérdés összefüggése a nemzeti biztonság vetületén kiemelten lényeges, hiszen a megfelelő biztonsági, védelmi szint garantálása szorosan összekapcsolódik békeidőben a biztonsági célú gazdasági, ipari teljesítménnyel/fejlesztésekkel, valamint a nemzetgazdaság védelmi és biztonsági célú felkészítésével, válsághelyzetben, konfliktusos időszakban pedig ennek eredményeként a védelmi gazdaság mozgósításával és volumenével áll összefüggésben. Ezen kérdések rendezésével kapcsolatos előremutató célkitűzések levezethetőek a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (a továbbiakban: Vbö.) IV. fejezetéből.

Fontos azonban kiemelni, hogy az előrejelzések sem lehetnek teljeskörűek, hiszen a külső környezet rendkívül dinamikus módon változhat. Erre egy aktuális példa az Orosz Föderáció által Ukrajna területén 2022 februárjában indított „különleges katonai művelet”, katonai agresszió, amely mind nemzeti, mind regionális, mind globális szinten nem várt hatásokat generál a katonai biztonság és a biztonság nem katonai összetevői terén is, akár az energiabiztonság, az élelmiszerellátás, a menekültek ellátásával kapcsolatos humanitárius, rendvédelmi és nemzetbiztonsági feladatok területén. Természetesen a fenti esemény Magyarországra gyakorolt várható hatásai kapcsán indokolt és szükséges a Stratégia felülvizsgálata a szövetségesi rendszereihez való kompatibilitás mentén, tekintettel például a 118. pontjára, miszerint „*Magyarország – miközben prioritásnak tartja a NATO és az EU kohéziójának megőrzését – érdekelt a magyar–orosz kapcsolatok és gazdasági együttműködés pragmatikus fejlesztésében*”. Magyarország törvényi szinten deklarált célja és alapvetése, hogy biztonsági jellegű kihívásai kapcsán az összehangolt védelmi tevékenységet és a válságkezelést a NATO Válságreagálási Rendszerével és az EU válságkezelési feladataival összhangban az eddigieknél még szorosabb módon biztosítsa, amelyet a Vbö. harmadik részében deklarál. De mi is az a Vbö…?

A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény nem átfogó stratégiai dokumentum, azonban előremutatóan az átfogó nemzeti biztonsági stratégiai célok megvalósulását hivatott keretbe foglalni, az általános „szkópot”, az intézményrendszert, az együttműködési kereteket, valamint a gazdasági folyamatokat harmonizálni, és az ehhez szükséges jogintézményeket törvényi szinten szabályozni. A Vbö-t a norma preambuluma szerint az Országgyűlés többek között *„Magyarország és a magyar nemzet védelme, biztonságának fenntartása, fejlesztése és ezekkel összefüggő érdekeinek érvényesítése, […] a 21. századi biztonsági környezet sokrétű és összetett kihívásainak és fenyegetéseinek kezelhetősége […]*” érdekében fogadta el és helyezi *pro futuro* 2023. július 1-jével hatályba, így biztosítva a szükséges felkészülési időt. Szenes Zoltán kutatási eredményei alapján[33] megállapítható, hogy a jogszabály többek között az új típusú kihívások és hibrid fenyegetések elleni fellépés reformfolyamataként azonosítható,

[32] Uo. p. 2.

[33] SZENES Zoltán: A hibrid fenyegetések elleni szakpolitika Magyarországon, Hadtudomány, 2021/4. pp. 39-56. ISBN: 978-963-531-615-1

amely folyamat aktuális harmadik szakasza az Alaptörvény 2020. december 22-ei kilencedik módosításával kezdődött.

A Vbö. 1. § bek. szerint „*Magyarország védelme és biztonsága nemzeti ügy, amelyen a nemzet fennmaradása és fejlődése, a közösségi és az egyéni jogok érvényesülése alapszik, ezért a magyar nemzet védelmével és biztonságának fenntartásával és fejlesztésével összefüggő jogszabályi rendelkezéseket e törvényre figyelemmel kell meghatározni*."[34] Ezen rendelkezés érvényre juttatása érdekében a honvédelem rendszerén, a rendvédelem és a rendvédelmi szervek mellett harmadik pillérként a nemzetbiztonsági szolgálatokat jelöli ki a jogszabály 3. §-a.[35] Szenes Zoltán szerint – összhangban a Vbö. preambulumával – a törvény Magyarország védelmi és biztonsági tevékenységének alapjaként megteremti az integrált, ágazatokon átívelő, az állami és nem állami szereplők közötti együttműködés keretében megvalósuló védelmi igazgatás átfogó normarendszerét. Azt, hogy a Vbö. szempontrendszerével mennyire azonosul a 2022. május 24-én megalakult ötödik Orbán-kormány, jelentősen kifejezi a miniszterelnök 2022. április 29-ei, Magyarország köztársasági elnöknek tett, kormányalakítással kapcsolatos integrált védelemkritikus nyilatkozata, miszerint „*Olyan kormány megalakítására teszek ígéretet, amely összességében és tagjaiban külön-külön is képes arra, hogy megvédje Magyarországot az előttünk álló veszélyes évtizedben is.*"[36] Szintén a külső nem várt regionális biztonsági kihívásokra kíván választ adni az Alaptörvény 2022. május 24-ei tizedik módosítása is, amely kiterjeszti a veszélyhelyzet rendkívüli jogrendjének kihirdethetőségét a kormány számára, a *„szomszédos országban fennálló fegyveres konfliktus, háborús helyzet vagy humanitárius katasztrófa […]"* esetére is, dinamikusan reagálva az ukrán-orosz konfliktus nemzeti biztonságot érintő váratlan fejleményeire.

A fentiek alapján tehát megállapítható, hogy az új típusú kihívások és a hibrid fenyegetések fokozódó térnyerése, valamint az azokra adandó optimális válaszok kialakítása átfogó biztonsági stratégiaaktualizáló, normaalkotó hatást váltott ki a jogalkotóból. A Vbö. általános indokolása szerint a jogszabály *„egy védelmi és biztonsági reformfolyamat*" alapja, amelyre hatálybalépéséig „*a transzatlanti térségben egyre jellemzőbb átfogó nemzetbiztonsági megközelítésre"*, illetve „*a NATO nemzeti ellenálló képesség fejlesztését célzó törekvéseire, valamint e témakörök hazai és külföldi tudományos elemzéseire"* alapozva felépíthetőek lesznek „*a technológia és a biztonsági környezet prognosztizálható változásaiból"* következő átfogó intézkedések és képességek. A preambulum szerint a törvény egy jelentős célja *„az átfogó megközelítés meghonosítása és megalapozása Magyarország védelme és a nemzet biztonságának szavatolása terén, amivel az ágazati sajátosságokat érintetlenül hagyva, az ágazati irányítás rendszerét továbbra is fenntartva, de a válságkezelésre való felkészülés és a válsághelyzeti működés koordináltságát fokozva, a válságkezelési szabályozást korszerűsítve, valamint a nem állami szereplők*

---

[34] A Vbö-ről a jogszabályi hierarchia vonatkozásában megállapítható, hogy *lex generalis* jellegben, magához „igazodónak" jelöli ki a védelmi és biztonsági tárgyú egyéb jogszabályokat, azaz rendelkezései egyfajta átfogó stratégiai keretet adnak, szinte primer normahierarchiai szinten.

[35] Vbö. 3. §

[36] https://kormany.hu/beszedek-interjuk/miniszterelnok/orban-viktor-sajtonyilatkozata-az-ader-janos-koztarsasagi-elnok-urral-tortent-egyezteteset-kovetoen (Letöltés ideje: 2022. 05. 01.)

felkészültségét és biztonságtudatosságát fokozva kívánja a jogalkotó megerősíteni hazánk és nemzetünk biztonságát." Fontos kiemelni, hogy a jogalkotó a törvény indokolásában a „*válságkezelés elengedhetetlen feltételeként"* azonosítja továbbá a dinamikusan változó külső környezethez való intenzív alkalmazkodási képesség kialakítását, amelyre tekintettel a normaalkotás részévé teszi az alkalmazkodási feltételek „*egyéni és össztársadalmi szinten történő*" biztosítását.[37] Kihangsúlyozandó, hogy a Vbö. általános indokolása a védelmi felkészülés központi szemléletébe emeli az „*átfogó nemzetbiztonsági megközelítés"*-t.

A védelem és biztonság nemzetbiztonsági szempontú megközelítésének fokozódó hangsúlyosságát alátámasztja a polgári nemzetbiztonsági szolgálatok irányításában 2022. május 25-én beállt közjogi változás is. A Miniszterelnöki Kabinetiroda 2022. május 13-ai sajtóközleménye[38] alapján az ötödik Orbán-kormány a külső biztonsági kihívások hatására újragondolta, optimalizálta a nemzetbiztonsági szolgálatok kormányzati irányítását. A közlemény szerint „*az új kormány legfontosabb feladata, hogy megőrizze Magyarország békéjét és biztonságát […] az említett cél érdekében meg kell erősíteni a miniszterelnök közvetlen munkaszervezetét; éppen ezért a polgári nemzetbiztonsági szolgálatok a jövőben a Miniszterelnöki Kabinetirodához tartoznak majd*". 2022. május 25-ei hatállyal a 182/2022 (V. 24.) Korm. rendelet 9. § (1) bek. alapján a Miniszterelnöki Kabinetirodát vezető miniszter a kormány polgári nemzetbiztonsági szolgálatok irányításért és polgári hírszerzési tevékenység irányításáért felelős tagja lett, mely feladatkört azt megelőzően elkülönítve a belügyminiszter, valamint a külgazdasági és külügyminiszter látta el. A Korm. rendelet 1. sz. mellékletének B) pontja szerint az Információs Hivatal, az Alkotmányvédelmi Hivatal[39], a Nemzetbiztonsági Szakszolgálat, valamint a 2022. május 25-én létrejövő új nemzetbiztonsági szolgálat[40], a Nemzeti Információs Központ kormányzati irányítása integrálásra került a Miniszterelnöki Kabinetirodát vezető miniszter hatáskörébe. A KNBSZ irányítását a kormány továbbra is a honvédelemért felelős miniszter útján látja el, tehát az elkülönül a polgári nemzetbiztonsági szolgálatokétól. Megállapítható, hogy az új irányítási struktúra összhangban van számos nemzetközi mintával, gyakorlattal. Például a német Szövetségi Hírszerző Szolgálat (BND[41]) irányítása a szövetségi Kancellár Hivatalának hatáskörébe tartozik.[42] Az Egyesült Királyságban a nemzetbiztonsági szolgálatok irányításáért a miniszterelnök felel.[43] Az Olasz Köztársaságban a nemzetbiztonsági szolgálatok irányítását szintén a kormányfő látja el.[44]

---

[37] Végső előterjesztői indokolás a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvényhez. Indokolások tára, 2021. július 01. 83. szám, p. 1210.

[38] https://kormany.hu/hirek/az-uj-kormany-legfontosabb-feladata-hogy-megorizze-magyarorszag-bekejet-es-biztonsagat (Letöltés ideje: 2022. 05. 13.)

[39] Az Nbtv. 1. § b) pontjának 2010. május 20-ai módosítását követően az Alkotmányvédelmi Hivatal a Nemzetbiztonsági Hivatal jogutódja.

[40] Az Nbtv. 1. § e) pontjának 2022. május 25-ei hatályú módosítása alapján a Nemzeti Információs Központ a Terroelhárítási Információs és Bűnügyi Elemző Központot kibővített hatáskörű jogutódja.

[41] Bundesnachrichtendiens

[42] Dr. Béres János (Szerk.): Külföldi nemzetbiztonsági szolgálatok; Zrínyi Kiadó, Budapest, 2018. p. 95. ISBN 978-963-12-9548-1.

[43] Uo. p. 107

[44] Uo. p. 172.

A nemzetbiztonsági ágazat stratégiai irányításának és szervezetrendszerének új kihívások, érdekek és értékek mentén történő mindenkori felülvizsgálata és újragondolása álláspontom alapján megfelel például a Vbö-ben is megjelenő biztonságkritikus alkalmazkodási képességnek, amelyet befolyásolnak mind a külső környezet, mind pedig a nemzeti szinten jelentkező egyes szakpolitikai, gazdasági, technológiai stb. hatások. Ezen álláspontot erősítik meg Barnóczki László és Kenedli-Tóth Eszter szerzőpáros legfrissebb kutatásai eredményei, miszerint „*A generális értelemben vett nemzetbiztonsági feladatok, az ezek végrehajtására hivatott szervezetek és ezek cselekvési rádiusza természetesen egy adott országon belül sem kőbe vésett, eleve elrendelt, megváltoztathatatlan axiómák, hanem az adott állam törvényhozása – és/vagy kormánya – által alakítható és alakítandó rendszer részei. A rendszer ideális esetben organikusan fejlődik, és módosulásai, illetve a rajta végrehajtott reformok a környező világ történéseire és jelenségeire, a külvilágból érkező fenyegetésekre és kihívásokra reagálnak*."[45]

Következtetések

Összefoglalva megállapítható, hogy a fentiekben elvégzésre került a hazai nemzeti biztonsági stratégiák evolúciójának vizsgálata – a részletes tartalmi elemzéstől eltekintve –, külön kitérve a nemzetbiztonsági szempontú rendelkezések áttekintésére, változásaira és a hatályos Stratégia kapcsán történő részletesebb elemzésére. Az átfogó stratégiai célkiűzések alakulásának és a nemzetbiztonsági ágazat biztonság garantálásában betöltött szerepének összefüggésében megállapítható, hogy a rendszerváltás óta eltelt időszak során számos változás következett be, amelyek reflektáltak az aktuális kihívásokra, szakpolitikai irányvonalakra és társadalmi elvárásokra. Például a hatályos Stratégia jóval hangsúlyosabb szerepet szán a kiberbiztonság és az offenzív reagáló képesség nemzetbiztonsági jellegű összefüggéseire, illeszkedve a kor technológiai jellegű biztonsági kihívásaihoz és lehetőségeihez.

Aktuális törvényalkotási szinten tapasztalhatóak azok a szakpolitikai irányok, amelyek ágazatokon átívelő összehangolt biztonsági, védelmi igazgatási rendszer megteremtését tűzték ki stratégiai célul 2023. július 01-ig. Integrálva az érintett szereplők képességeit, funkcióit, jelentős szerepet szánva, egyfajta transzatlanti megközelítésben a nemzetbiztonsági szolgálatoknak, így reagálva a 21. század új típusú, hibridjellegű kihívásaira, a kormány alkotmányos jogalapjának kiterjesztésével a védelem hatékony megszervezése érdekében. A folyamatban lévő és várható normaalkotási irányok, szakpolitikai döntések alapján már előrevetíthető a nemzetbiztonsági ágazat egyre kiemeltebb szerepe a biztonság garantálásának területén. Kijelenthető, hogy a nemzetbiztonsági szervezetrendszer számára az átfogó stratégiai célok végrehajtáshoz szükséges intézkedések és eszközök ágazati tervezési dokumentumszintű definiálása egyre aktuálisabbá válik.

Megállapítható, hogy 2022-re az aktuális és nem várt biztonsági kihívások a polgári nemzetbiztonsági szolgálatok kormányzati irányításának újragondoláshoz, optimalizálásához vezettek, amelyet jellemez a 2022. május 24-én újonnan megalakult kormány tárgykört érintő szinte azonnalos normaalkotási tevékenysége is.

[45] BARNÓCZKI – KENEDLI-TÓTH. i. m. p. 72.

A folyamat eredményeként kiemelendő, hogy 2022. május 25-ei hatállyal a Miniszterelnöki Kabinetiroda szervezetébe tagozódó polgári nemzetbiztonsági szolgálatok irányítását a kormány integráltan látja el az azt vezető miniszter útján, a korábbi elkülönült struktúrát felváltva. Ezen szervezési elv megfelel számos nemzetközi gyakorlatnak. A döntés jelzi a nemzetbiztonsági szolgálatok egyre kiemeltebb szerepét a nemzeti szuverenitás, biztonság garantálása érdekében meghozandó döntések előkészítése terén. A nemzetbiztonsági ágazatnak fokozottabb hangsúlyosságát mutatja azon változás is, miszerint átfogó tárcaközi szinten 2020. május 25-ei hatállyal, a Nemzetbiztonsági Kabinet kibővített hatáskörű jogutódjaként, létrehozásra került a Védelmi Tanács, amely elnöke a kormányfő lett, az ehhez szükséges közigazgatási háttér-szervezetrendszer[46] támogatásával. A miniszterelnök számára így biztosítottá vált a nemzetbiztonsági szolgálatok tevékenységének összkormányzati szintű közvetlen koordinálása, várhatóan így professzionalizálva és maximalizálva a nemzetbiztonsági ágazat hatékonyságát és eredményes hozzájárulását a biztonság egyes összetevőinek komplex érvényesüléséhez.

Felhasznált irodalom:

- BARNÓCZKI László – KENEDLI-TÓTH Eszter: A nemzetbiztonsági szolgálatok megszervezése és működése az eltelt harminc év során – változások az ágazatot érő legfontosabb kihívások tükrében; In: CHRISTIÁN László – LIPPAI Zsolt – NÉMETH Zsolt (Szerk.): A rendszerváltás hatása a rendészetre; Ludovika Egyetemi Kiadó, Budapest, 2021. pp. 71-102. ISBN 978-963-531-554-3
- CSIKI Tamás: Az új Nemzeti Katonai Stratégia a nemzetközi tapasztalatok tükrében; Nemzet és Biztonság, 2014/2. pp. 45-61. ISSN 1789-5286
- CSIKI VARGA Tamás – TÁLAS Péter: Magyarország új nemzeti biztonsági stratégiájáról; Nemzet és Biztonság, 2020/3. pp. 89-112. ISSN 1789-5286
- DOBÁK Imre – TÓTH Tamás: A külső környezet, és tendenciák nyomon követésének szükségessége a stratégiaalkotás tükrében; In: (szerk): Stratégiák, stratégiai gondolkodás, nemzetbiztonság, TKP2020-NKA-09, Budapest, 2022, Ludovika Egyetemi Kiadó. ISBN (Megjelenés alatt.)
- DR. ALMÁSI Ferenc alezredes: Honvédelmünk NATO integrációs folyamatának áttekintése, tapasztalatai és következtetései jogi szempontból; Doktori (PhD) értekezés, ZMNE HDI, Budapest, 2005.
- DR. BÉRES János (Szerk.): Külföldi nemzetbiztonsági szolgálatok; Zrínyi Kiadó, Budapest, 2018. ISBN 978-963-12-9548-1
- FITZSIMMONS, Michael: Scenario Planning And Strategy In The Pentagon; Strategic Studies Institute US Army War College, Pennsylvania, 2019. ISBN 158-487-801-1

[46] 1144/2010. (VII. 7.) Korm. határozat 58. pont (1) bek. A Nemzetbiztonsági Munkacsoport, valamint a Honvédelmi és Rendészeti Munkacsoport a Védelmi Tanács döntés-előkészítő testülete.

- IGNÁTH Éva: Az Országgyűlés 94/1998. (XII. 29.) sz. határozata a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről; Grotius, 2009.
- KENEDLI Tamás: A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években; Nemzetbiztonsági Szemle, 2020/1. pp. 74-94. ISSN 2064-3756
- KISS Petra: A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében; Hadtudomány, 2012/3-4. pp. 68-79. ISBN: 978-963-531-615-1
- KUN SZABÓ István vezérőrnagy – SANDRA Sándor ny. o. ezredes – STICZ László ezredes: Haza, biztonság, honvédelem, haderőfejlesztés; Honvédségi Szemle, 2018/5. pp. 139-148. ISSN 2060-1506
- SABJANICS István: A nemzetbiztonság jogi koncepciója; In: CSINK Lóránt (Szerk.): A nemzetbiztonság kihívásainak hatása a magánszférára; Pázmány Press, Budapest, 2017. pp. 103-124. ISBN 978-963-308-319-2
- SZENES Zoltán: A hibrid fenyegetések elleni szakpolitika Magyarországon; Hadtudomány, 2021/4. pp. 39-56. ISBN: 978-963-531-615-1
- TÁLAS Péter: A nemzeti katonai stratégia és a magyar stratégiai kultúra; Hadtudomány, 2013/3-4. pp. 14-28. ISBN: 978-963-531-615-1
- TEKE András: A rendészet/rendvédelem tartalmi és funkcionális megjelenítése a magyar (nemzeti) biztonsági stratégiákban/stratégiai dokumentumokban (1993-2020); Határrendészeti tanulmányok, 2021/3. pp. 84-132. ISSN 2061-3997
- The Alliance's Strategic Concept. 1999. április 24. Press Release NAC-S(99) p. 65. https://www.nato.int/cps/en/natohq/official_texts_27433.htm (Letöltés ideje: 2022. június 4.)

Internetes hivatkozások:

- Orbán Viktor sajtónyilatkozata az Áder János köztársasági elnök úrral történt egyeztetését követően, Magyarország Kormánya; 2022. 04. 19. https://kormany.hu/beszedek-interjuk/miniszterelnok/orban-viktor-sajtonyilatkozata-az-ader-janos-koztarsasagi-elnok-urral-tortent-egyeztetest-kovetoen (Letöltés ideje: 2022.05.01.)
- Az új kormány legfontosabb feladata, hogy megőrizze Magyarország békéjét és biztonságát, Magyarország Kormánya; 2022. 05. 13. https://kormany.hu/hirek/az-uj-kormany-legfontosabb-feladata-hogy-megorizze-magyarorszag-bekejet-es-biztonsagat (Letöltés ideje: 2022.05.13.)

Jogforrások:

- Magyarország Alaptörvénye (2011. április 25.)
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
- 1999. évi I. törvény a Magyar Köztársaságnak az Észak-atlanti Szerződéshez történő csatlakozásáról és a Szerződés szövegének kihirdetéséről

- 1999. évi LVIII. törvény a Magyar Köztársaságnak az Észak-atlanti Szerződéshez történő csatlakozásáról és a Szerződés szövegének kihirdetéséről szóló 1999. évi I. törvény módosításáról
- 182/2022. (V. 24.) Korm. rendelet a Kormány tagjainak feladat- és hatásköréről
- 11/1993. (III. 12.) OGY határozat a Magyar Köztársaság biztonságpolitikájának alapelveiről
- 227/1993. (IV. 23.) OGY határozat a Magyar Köztársaság honvédelmének alapelveiről
- 94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről
- 2144/2002. (V. 6.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról
- 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról
- 1144/2010. (VII. 7.) Korm. határozat a Kormány ügyrendjéről
- 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 1393/2021 (VI. 24) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról
- 1260/2022. (V. 24.) Korm. határozat a Kormány ügyrendjéről szóló 1144/2010. (VII. 7.) Korm. határozat módosításáról
- 57/2016. (XI. 24.) HM-MvM-BM-KKM együttes utasítás a Nemzeti Biztonsági Stratégia felülvizsgálatára létrehozott munkacsoportról
- A külügyminisztertől Közlemény a Washingtonban, 1949. április 4-én létrehozott Észak-atlanti Szerződésnek a Magyar Köztársaság vonatkozásában történt hatálybalépéséről. Magyar Közlöny, 1990/25. sz. 1999.03.26. 1760. o.
- Végső előterjesztői indokolás a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvényhez. Magyar Közlöny Indokolások Tára, 2021. július 01. 2021 évi 83. sz. pp. 1210-1221.

NEUSPILLER FERENC

A NATO „LEGGYENGÉBB LÁNCSZEME”? OLASZORSZÁG KATONAPOLITIKAI HELYZETE 1963-1975.

Bevezetés

A hidegháború korszakában az 1960-as és az 1970-es évtizedeket az enyhülés jellemezte. A korábbi feszült viszony után a két szemben álló szuperhatalom, a Szovjetunió és az Egyesült Államok, és a két szemben álló katonai tömb, a Varsói Szerződés és a NATO megkezdte a tárgyalásokat a fegyverzetkorlátozásról, illetve -csökkentésről. Mivel Olaszország a NATO egyik alapítótagja volt, ezért ezek a tárgyalások természetesen Rómát is érintették. Mindeközben azonban az olasz haderőt fel kellett volna készíteni arra, hogy egy esetleges ellenséges támadást mind a szárazföldön, mind a tengeren, mind a levegőben képes legyen megállítani, amit jelentősen hátráltatott az ország instabil belpolitikai helyzete, a folyamatos kormányválságok és az olasz gazdaság állapota. Ebben a meglehetősen bonyolult katonapolitikai helyzetben Olaszország legfőképp az Egyesült Államokra és a NATO-ra támaszkodhatott. A szövetségben betöltött szerepét viszont jelentősen hátráltatta, hogy több magyar nagykövetségi jelentés szerint is Olaszországot a lassan stabilizálódó gazdasága, a társadalmi feszültség és a Nyugat-Európában az egyik legerősebb kommunista párt miatt a NATO leggyengébb tagjának tekintették. A kijelentés valóságtartalmának megvizsgálása során kiderül az is, hogy milyen kihívásokkal kellett a NATO-nak és Olaszországnak szembenéznie az 1963 és 1975 közötti időszakban.

Olaszország belpolitikai helyzete

A hidegháború korában Olaszország NATO-ban betöltött szerepére, katonapolitikai helyzetére és hadászati lehetőségeire három tényező hatott döntően: az ország belpolitikai helyzete, gazdasági állapota és földrajzi elhelyezkedése.

A második világháború utáni évtizedekben Olaszországot folyamatos belpolitikai válságok jellemezték. Annak ellenére, hogy a kor legerősebb pártja, a Kereszténydemokrata Párt (Democrazia Cristiana-DC) rendre megnyerte a választásokat, és így a kormányalakítás lehetőségét is, a párt politikusai közül kikerülő miniszterelnökök nem tudtak olyan kormányt létrehozni, amely hosszabb időn keresztül képes lett volna irányítani az országot. A belpolitikai stabilitás megteremtésének érdekében Aldo Moro 1963 decemberében megalakította első középbal kormányát, amelyben – keresztényemokrata, szociáldemokrata és republikánus képviselőkön kívül – a korábbi szokásoktól eltérően már több szocialista politikus is helyet kapott.[1] Igaz, Moro első kormánya alig több mint fél év után a belső

[1] Magyar Nemzeti Levéltár Országos Levéltára (MNL OL) XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében. A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. pp. 5-6.

feszültségek és ellentétek miatt megbukott, de 1964 júliusában megint a kereszténydemokrata politikus kapott kormányalakítási megbízást, így a középbal maradt hatalmon.[2]

A középbal azonban nem hozta el a várva-várt belpolitikai stabilitást, amelynek egyik bizonyítéka, hogy 1968 és 1972 között Olaszországban hat kormányválság is volt. Ezt követően Giulio Andreotti lett a miniszterelnök, aki jobboldali fordulatot kívánt végrehajtani, ebbe a kísérletébe azonban alig egy év elteltével belebukott, így 1973-tól megint a középbal volt hatalmon.[3] Miközben ráadásul az 1960-as évek végétől a DC folyamatosan veszített népszerűségéből (az 1968-as választáson 39%-os eredményt ért el[4], 1972-ben 38,4%-os, az 1975-ös tartományi választáson pedig már csak 35,3%-os eredményt tudott felmutatni), addig a kommunista párt (Partito Comunista Italiano – PCI) folyamatosan erősödött (1968-ban a PCI a szavazatok 26,9%-át kapta, 1972-ben már 28,3, az 1975-ös tartományi választáson pedig már 33,4% eredménnyel zárt).[5]

A választásokon elért eredmények ismeretében nem meglepő, hogy az 1970-es években felvetődött a DC és a PCI közötti kiegyezés lehetősége, a történelmi kompromisszum („*compromesso storico*"). A történelmi kompromisszum megkötésének lehetőségét növelte, hogy a PCI főtitkára, Enrico Berlinguer az 1968-as csehszlovákiai események hatására szembefordult a Szovjetunióval,[6] 1972 decemberétől pedig egy a korábbiaknál konstruktívabb politikába kezdett, amelynek jeleként a PCI részt vett az európai parlamentben, és szorosabb kapcsolatot kezdett kialakítani a nyugat-európai szocialista pártokkal.[7] De a két nagy párt egymáshoz való közeledése, és az a lehetőség, hogy kommunisták bekerülnek az olasz kormányba, aggodalommal töltötte el a NATO-tagállamok vezetőit, elsősorban az Egyesült Államok elnökét. Nixon Watergate-botránnyal összefüggő lemondása miatt[8] az 1974 nyarára halasztott washingtoni tárgyaláson az amerikai elnök, Ford kijelentette az olasz köztársasági elnöknek, Leonénak, hogy „*Az amerikaiak kategorikusan összeegyeztethetetlennek tartják a NATO érdekeivel a kommunisták belépését a kormányba"*.[9]

Az 1960-as és az 1970-es években Olaszország belpolitikai problémáit tovább súlyosbították a terrorista támadások s az államcsíny-kísérletek. 1969. április 25-én, az olasz felszabadulás napján bomba robbant Milánóban, 5 embert megsebesítve, nem sokkal a robbanás után pedig egy másik, fel nem robbant bombát is találtak a

---

2 TRANFAGLIA, Nicola: Anatomia dell'Italia repubblicana 1943-2009. Passigli Editori, Firenze, 2010. pp. 101-102.

3 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 8.

4 SZABÓ Tibor: Olaszország politikatörténete 1861-2011. Belvedere Meridionale, Szeged, 2012. p. 125.

5 MAMMARELLA, Giuseppe – CACACE, Paolo: La politica estera dell'Italia. Dallo stato unitario ai gorni nostri. Editori Laterza, Róma, 2010. p. 390.

6 TRANFAGLIA i. m. p. 122.

7 MAMMARELLA – CACACE i. m. p. 357.

8 MAGYARICS Tamás: Az Amerikai Egyesült Államok története, 1914-1991. Kossuth Kiadó, Budapest, 2008. pp. 153-155.

9 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Jelentés, Róma, 1974. október 11. p. 2.

városban. A merénylet csak a kezdete volt egy sorozatnak, amely az ólomévek („*anni di piombo*") néven vált ismerté. A szélsőjobboldali és szélsőbaloldali terrorszervezetek által végrehajtott akcióknak 1969 és 1982 között összesen 350 halálos áldozata volt.[10] Ezek közül talán a legsúlyosabb 1969. december 12-én történt, amikor kevesebb, mint egy óra leforgása alatt a két legnagyobb olasz városban, Rómában és Milánóban is történtek merényletek. 16 óra 37 perckor Milánóban, a piazza Fontanán a Banca Nazionale dell'Agricoltura épületénél volt az első robbanás, amelyben 17-en meghaltak és további 88-an megsebesültek. Nem sokkal később, szintén Milánóban a piazza della Scalán a Banca Commerciale Italiana közelében találtak egy fel nem robbant bombát. A következő bomba 16.55-kor robbant Rómában, a Banca Nazionale del Lavoro közelében 13 ember sérülését okozva, majd 17 óra 20 és 30 perc között további két merénylet történt, az egyik az Altare della Patria közelében, a másik a piazza Venezián, a Museo del Risorgimento bejáratánál, négy ember sebesülését okozva.[11]

Az 1960-as és 1970-es években több államcsíny-kísérletre is fény derült. Ezek közül az egyik legismertebb az Arma dei carabinieri vezetőjéhez, Giovanni de Lorenzóhoz köthető Piano Solo. A Moro-kormány válságának az idején, 1964 nyarán De Lorenzo, aki korábban az olasz fegyveres erők titkosszolgálatának (Servizio Informazioni Forze Armate – SIFAR) a főnöke volt, és ebben az időben is nagy befolyással bírt a szolgálatra azt tervezte, hogy a baloldal túlzott megerősödése esetén fegyveres hatalomátvételt hajt végre, ami után a PSI-vel való együttműködés lezárásaként egy jobbközép kormányt állítana fel.[12] Néhány évvel de Lorenzo után az akkor már SID (Servizio Informazioni Difesa) néven működő titkosszolgálat másik vezetője is botrányba keveredett. 1970. december 7-ről 8-ra virradó éjszaka egy szélsőjobboldali szervezet, az Avanguardia nazionale tagjai azt tervezték, hogy elfoglalják az olasz Belügyminisztérium épületét. Az utolsó pillanatban lefújt államcsíny legfőbb alakja az MSI[13] tiszteletbeli elnöke, a „Fekete Herceg"-ként ismert Valerio Borghese volt.[14] A végül meghiúsult államcsíny közben a SID vezetője,Vito Miceli furcsa, érthetetlen viselkedésével hívta fel magára a figyelmet. Amikor kiderült, hogy az Avanguardia nazionale tagjai már a Belügyminisztérium épületében tartózkodnak, Miceli éjfél körül azt hazudta a munkatársainak, hogy már megkezdte az intézkedést, ezzel lehetőséget adott a puccsistáknak a menekülésre.[15]

Vito Micelit 1974. október 31-én a padovai bíróság elé állították államellenes fegyveres összeesküvés elkövetésének vádjával, miközben a milánói bíróság hasonlóra készült Henke admirális nyugalmazott vezérkari főnökkel szemben, aki

---

[10] MAMMARELLA – CACACE i. m. p. 329.

[11] BUTTIGNON, Ivan – ZENONI, Mattia: M.S.I. e terrorismo nero tra verità e montature. I collateralismi tra il partito neofascista e le organizzazioni armate di estrema destra; Solfanelli, 2014. pp. 168-169.

[12] DE LUTIIS, Giuseppe: I servizi segreti in Italia. Dal fascismo alla seconda repubblica; Editori Riuniti, Róma, 1998. pp. 71-73.

[13] Az MSI (Movimento Sociale Italiano – Olasz Szociális Mozgalom) egy újfasiszta párt volt a második világháború utáni Olaszországban. Az MSI-ről magyar nyelven lásd: CHIARINI, Roberto: A Movimento Sociale Italiano – történeti áttekintés; In: FEITL István (Szerk.): Jobboldali radikalizmusok tegnap és ma; Napvilág Kiadó, Budapest, 1998. pp. 89-113.

[14] PACINI, Giacomo: Il cuore occulto del potere. Storia dell'Ufficio Affari riservati del Viminale (1919-1984); Nutrimenti, Róma, 2011. pp. 206-207.

[15] BUTTIGNON – ZENONI i. m. pp. 69-70.

Miceli elődje volt a SID élén. Andreotti azzal magyarázta Miceli letartóztatását, hogy akadályozta a Fontana téri robbantás vizsgálatának lefolytatását. A nyomozás során a milánói, padovai, torinói és római bíróságok anyagokat gyűjtöttek a SID-ről, amelyekből kiderült, hogy a szervezet vezetői tudtak a fasiszta terrorcsoportok által szervezett összeesküvésekről, robbantásokról, merényletekről, sőt, tisztjeik útján személyesen képviseltették magukat ezek végrehajtásában. A Miceli elleni tárgyalás kulcsfigurája Giuseppe Condo alezredes, a SID munkatársa volt, vagy inkább lett volna. Condo ugyanis nem sokkal a kihallgatása előtt, 1974. november 12-én, 42 évesen meghalt. Boncolása utáni orvosi jelentésében csak annyi szerepel, hogy halálának az oka a szívműködés megállása volt. A római magyar nagykövetség szerint Condo rejtélyes halála kísérteties hasonlóságot mutat Renzo Rocca halálával, akinek az 1964-es SIFAR-botrányt követően kellett volna tanúskodnia. Olasz lapértesülések szerint mindeközben Kissinger személyesen járt Morónál Miceli ügyében, ugyanis a SID korábbi vezetője ismerte a nyugati hírszerzés és kémelhárítás rendszerét, és attól félt, hogy a NATO-val és a CIA olaszországi tevékenységével kapcsolatos titkokat mondhat el.[16] Ahogy azt Giovanni de Lorenzo és Vito Miceli esete bizonyítja, az 1960-as és az 1970-es években a terrorista támadásokba és az államcsíny-kísérletekbe gyakran az olasz fegyveres erők titkosszolgálatainak vezetői is belekeveredtek, tovább súlyosbítva a belpolitikai válságot, és aláásva a fegyveres szolgálatokba vetett bizalmat.

Az olasz gazdaság

Az állandó belpolitikai problémák és kormányválságok ellenére az 1950-es és az 1960-as években Olaszország gazdasága folyamatosan fejlődött. Ebből a korszakból is kiemelkedett az 1955 és 1963 közötti időszak. A „gazdasági csoda" korszakában Olaszország gazdasági növekedése évi 6-8% között volt, jelentős ipari fejlődés ment végbe elsősorban a Torino–Milánó–Genova háromszögben, ami hozzájárult a déli területeket sújtó munkanélküliség csökkenéséhez, hiszen az itteni gyárakban főleg déli munkaerőt alkalmaztak. A második világháború utáni időszakhoz képest modernizálódott a termelési szerkezet, ami hozzájárult a mezőgazdaságban dolgozók számának folyamatos csökkenéséhez, és az iparban és szolgáltatási szektorban dolgozók számának növekedéséhez. Az 1960-as évekre megvalósult Olaszországban a „jóléti állam", ami megmutatkozott a tömegfogyasztásban is.[17]

Ez a gazdasági fejlődés azonban nem kis részben a külföldi tőke beáramlásának volt köszönhető. A magyar belügyi hírszerzéshez egy „Von Schiller" fedőnevet használó, Olaszországban dolgozó újságírótól olyan információk jutottak el, miszerint 1946 és 1960 között az USA összesen mintegy 3,4 billió dollár tőkét helyezett el Olaszországban, amelynek 70 százalékát gyáriparra, vasúti fejlesztésekre és közmunkákra fordították. Az USA-n kívül Hollandia, Belgium, Kanada és az NSZK is jelentős összegeket fordított az olasz gazdaságba. Az amerikai beruházások nagyobb politikai, gazdasági, társadalmi vagy katonai befektetésként jelentek meg Olaszországban, amelyekből elsősorban az olaj és bányászat, a kémia és

[16] MNL OL XIX-J-1-j Olaszország KÜM TÜK 1975/110. doboz – Jelentés, Róma, 1975. március 8. pp. 1-5.
[17] SZABÓ i. m. pp. 114-115.

gyógyszeripar, az acélipar, illetve az elektronika részesedett. Közben olasz gazdasági szakemberek rendszeresen vettek részt tanulmányutakon amerikai egyetemeken vagy gyárakban. Ezek mellett kiemeli, hogy a FIAT, a Banca Commerciale és a Banca di Santo Spirito is élvezi amerikai magánbefektetők támogatását. Ezek munkásságát egészítették ki a különböző befektetési alapok, amelyek leginkább Johnson ideje alatt voltak jellemzőek, és amikből Róma, Milánó, illetve Torino részesedett, miközben katonai befektetések is érkeztek az országba, például a NASA-tól. „Von Schiller" arról értesült, hogy 1967-ben Washington 160 millió dollár tőkével hatolt be az olasz gazdaságba, amit ki kell egészíteni a befektetési alapokból, a Közös Piactól vagy a Vatikánon keresztül érkező további 560 millió dollárral,[18] miközben az 1960-as évek elején a kezdődő gazdasági válságból csak a Johnson amerikai elnöktől kapott 1 milliárd dolláros hitel tudta kihúzni Olaszországot, amit a Nemzetközi Valutaalap további 225 millió dollárral egészített ki.[19]

Az Egyesült Államoktól és a Nemzetközi Valutaalaptól kapott hitel már jelezte, hogy a fejlődés ellenére az olasz gazdaság instabil volt. Ráadásul az 1960-as évek második felében a gazdasági fejlődés lelassult, az 1970-es évek elején pedig Olaszország gazdaságát a világháború vége óta a legnagyobb válság sújtotta. Nixon amerikai elnök 1971. augusztus 15-én „új gazdaságpolitikát" jelentett be, amelynek keretein belül az amerikai fizetési mérleg és a dollár védelmében felfüggesztette a dollár aranyra válthatóságát, és 10%-os pótadót vezetett be az importra. Ez a nixoni „új gazdaságpolitika" válságba taszította a nemzetközi pénzügyi rendszert, ami néhány évvel később Olaszországban is éreztette hatását. Ezt a válságot mélyítette az 1973-as olajválság, amikor az olajkitermelő országok szervezete, az OPEC drasztikus olajár-emelést hajtott végre, ami hozzájárult a nyersanyagok árának megugrásához[20] Az amúgy is komoly nyersanyaghiánnyal küszködő Olaszország számára az 1973-as olajválság a gazdaság összeomlását jelentette, ami hozzájárult a munkanélküliség és az infláció növekedéséhez. Jól mutatja az ország problémáját és a gazdaság helyzetét, hogy az infláció 1973 és 1974 között 10,4%-ról 19,4%-ra emelkedett.[21]

A NATO déli szárnya az 1960-as és 1970-es években

A folyamatos belpolitikai válságok és a gazdasági problémák miatt Olaszország egyedül a földrajzi helyzetére támaszkodva tudta növelni szerepét a NATO-n belül. Mivel azonban a Szövetség abból a felvetésből indult ki, hogy egy, a Varsói Szerződés által indított hadműveletben a főerők az észak-német síkságon keresztül fognak támadni,[22] ezért Olaszország legfeljebb mellékhadszíntér lenne, ami jelentősen csökkentette az ország súlyát.[23]

---

[18] Állambiztonsági Szolgálatok Történeti Levéltára (ÁBTL) 3.2.3 Mt-867/2. p. 34-37. Információs jelentés, Róma, 1968. június 15.

[19] MAMMARELLA – CACACE i. m. p. 219.

[20] HORVÁTH Jenő – PARAGI Beáta – CSICSMANN László: Nemzetközi kapcsolatok története 1941-1991; Antall József Tudásközpont, Budapest, 2014. pp. 226-227.

[21] MAMMARELLA – CACACE i. m. p. 231.

[22] VALKI László (szerk): A NATO. Történet, szervezet, stratégia, bővítés; Corvina Kiadó, Budapest, 1999. p. 47.

[23] MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 16.

Az Egyesült Államoknak és a NATO-nak viszont szüksége volt Olaszországra, hogy a Földközi-tenger keleti medencéjében meg tudják alapozni az amerikai jelenlétet, és fenn tudják tartani a korábban kialakult status quót. Olaszországnak pedig szüksége volt a NATO-ra, hogy alacsony hadi kiadások mellett is képes legyen megteremteni a félsziget hosszú távú biztonságát.[24] Ráadásul az 1960-as évek közepén Franciaország kilépésével a NATO katonai szervezetéből Olaszország szerepe felértékelődött a Földközi-tenger védelmében. A Szövetségen belül már 1963 óta feszültség volt, ugyanis De Gaulle ellenezte azt a tervet, ami az önálló brit és francia atomarzenált bevonta volna a többnemzetiségű MLF-be (Multilateral Forces), és saját nukleáris ütőerő, a „force de frappe" kialakítására törekedett. A Tábornok már 1965 januárjában kijelentette, hogy véget kell vetni a francia haderők integrációjának, és valamennyi külföldi katonát el kell távolítani Franciaországból.[25] Mivel a feszültséget nem sikerült enyhíteni, ezért 1966. február 21-én egy sajtóértekezleten De Gaulle bejelentette, hogy Franciaország kilép a NATO katonai szervezetéből, a francia egységeket kivonja az atlanti fegyveres erők állományából, tisztjeit visszahívja a NATO-törzsből, és megszünteti az országban lévő külföldi támaszpontokat.[26]

Franciaország kilépésének komoly következményei voltak, hiszen de Gaulle nem csak tengeri erőit vonta ki a szövetség kötelékéből, de csökkentette szárazföldi és légi egységeinek számát is a NATO kötelékén belül, előbbit 5-ről 2-re, utóbbit 35-ről 15-re, és félő volt, hogy az integrált légvédelem rendszeréből is kilép (bár ez utóbbi végül nem valósult meg). Ráadásul jó pár NATO-intézmény működött Franciaországban, mint például az Atlanti Tanács, az Európai Főparancsnokság, vagy a Védelmi Kollégium, amiket a francia területen állomásozó amerikai csapatokkal és támaszpontokkal együtt ki kellett telepíteni. Ezeknek jelentős részét végül az NSZK-ba, a Benelux államokba, Spanyolországba és Olaszországba helyezték át, amik növelték ezeknek az országoknak a szerepét a szervezeten belül. Utóbbit még a nukleáris fegyverekkel foglalkozó Állandó Csoportba is meghívták, ami egyértelmű jele volt annak, hogy az USA nagyobb szerepet kíván szánni az olaszoknak.[27]

Miközben a NATO-n belül feszültség volt de Gaulle politikája miatt, közben a Szovjetunió jelentős flottaépítésbe kezdett. Az 1960-as években Gorskov tengernagy igyekezett a korábbi tengerparti szovjet flottát óceánivá átalakítani, hogy sikerüljön közvetlenebb kapcsolatot megteremteni a négy szovjet flotta között. Ennek köszönhetően a Szovjetunió figyelmének előterébe került például a Fekete-tenger, a Boszporusz, a Szuezi-csatorna és a Földközi-tenger.[28] A szovjet flotta jelenléte a Földközi-tenger térségében nem csak felértékelte a terület stratégiai szerepét, de

---

[24] HORVÁTH Jenő: Követő külpolitika. Az olasz EUrópa-politika a második világháború után. In: KISS J. László (Szerk.): A tizenötök Európái. Közösségi politikák – nemzeti politikák; Osiris Kiadó, Budapest, 2000. p. 246.

[25] SHENNAN, Andrew: De Gaulle; Akadémiai Kiadó, Budapest, 1997. pp. 140-142.

[26] GAZDAG Ferenc: Franciaország története 1945-1995. Zrínyi Kiadó, 1996. pp. 116-117.

[27] Istituto Luigi Sturzo Archivio Giulio Andreotti (ILS AGA) NATO series Memorandum by General Staff of Defense (SMD) to the Minister, NATO reorganization, 1965. december 29. p. 12. https://digitalarchive.wilsoncenter.org/document/165226 (Letöltés ideje: 2022. 04. 19.)

[28] FISCHER Ferenc: A megosztott világ. A Kelet-Nyugat, Észak-Dél nemzetközi kapcsolatok fő vonásai 1941-1991.; Budapest, 1996. pp. 244-248.

csökkentette a 6. amerikai flotta beavatkozási lehetőségeit, és komoly veszélybe sodorta tengeri ellenőrzését is.[29]

Franciaország kilépése és a szovjet flotta fejlesztése miatt, alkalmazkodva a belső és külső körülményekhez, az 1960-as évek második felében döntés született a NATO átszervezéséről. Az átszervezés során meggyorsították a NATO légvédelmi rendszerének kialakítását (NATO Air Defence Ground Environment – NADGE), amelyet hozzákapcsoltak a SATCOM-hoz.[30] Ennek olaszországi központja a borge piavei légitámaszponton volt.[31] A szovjet terjeszkedés miatt a NATO-ban döntés született a földközi-tengeri erők jelentős növeléséről, a melyhez Olaszország ejtőernyős és tengerészeti alakulatokkal igyekezett hozzájárulni, és belekezdtek az anconai kikötő fejlesztésébe is,[32] illetve a nápolyi székhelyű AFSOUTH[33] rakétakilövő-hajókkal, tengeralattjáró-elhárítókkal és repülőgépekkel erősödött.[34] Ezek az átszervezések és erősítések hozzájárultak ahhoz, hogy az 1960-as évek végére Olaszország aktívabb, nagyobb szerepet tudjon betölteni a NATO-n belül.

Szovjet haderőfejlesztés és a NATO válasza

Az olasz haderőfejlesztés szükségességét megerősítették a NATO Védelmi Tervező Tanácsának 1972. május 24-i brüsszeli ülésén elhangzottak, amelyen felhívták a tagállamok figyelmét arra, hogy a Varsói Szerződés részéről fenyegetés várható, amelyet alátámasztanak a Szovjetunió mind mennyiségi, mind minőségi katonai expanziójáról szóló hírek.[35] Az ülésen előterjesztettek egy jelentést, ami szerint a Szovjetunió és a Varsói Szerződés folyamatosan növeli katonai erejét és kapacitását, és kihangsúlyozták, hogy stratégiai téren a Szovjetunió az elmúlt években figyelemreméltó eredményeket ért el, aminek köszönhetően minimum utolérte a Nyugatot, de bizonyos szempontból még meg is előzte azt. A jelentésben részletezték, hogy a Szovjetunió összesen nagyjából 1400 interkontinentális ballisztikus rakétával (Intercontinental Ballistic Missile – ICBM) rendelkezik, amely körülbelül egyharmaddal múlja felül az Egyesült Államok 1054 hasonló rakétáját. Légierő szempontjából a Szovjetunió egyelőre kevesebb hosszútávú bombázóval rendelkezik, mint az Egyesült Államok, de folyamatosan fejlesztenek új konstrukciókat, amelyek várhatóan 2-3 éven belül elkészülnek. A szovjet légierőnek összesen 11.500 egysége van, amit kiegészít a Varsói Szerződés tagállamainak 2500 repülője.

---

[29] MINOLFI, Salvatore: Italia, Europa e Stati Uniti: La NATO dal 1969 al 1989; In: MINOLFI, Salvatore (Szerk.): L'Italia e la NATO. Una politica estera nelle maglie dell'alleanza; CUEN, Nápoly, 1993. p. 104.

[30] A SATCOM (Satellite Communications) a műholdas összeköttetések rendszere. Lásd: KERESZTY András: Tények könyve: NATO; Greger-Delacroix, Budapest, 1997. p. 20.

[31] ÁBTL 3.2.3. Mt-867/2. p. 70. – Jelentés, Róma, 1968. július 10.

[32] ÁBTL 3.2.3. Mt-867/2. p. 80. – Jelentés, Róma, 1968. július 10.

[33] Az AFSOUTH (Allied Forces Southern Europe) a dél-európai szövetséges erők elnevezése. Lásd: KERESZTY i. m. p. 16.

[34] ÁBTL 3.2.3. Mt-867/2. p. 104. – Információs jelentés, Róma, 1968. november 13.

[35] ILS AGA NATO series Memorandum by Cheef of Defense Staff, „Political- military considerations with regards to the ministerial meeting of the NATO Defense Planning Committee" (DPC), Brüsszel, 1972. május 24. pp. 1-2. https://digitalarchive.wilsoncenter.org/document/145154 (Letöltés ideje: 2022. 04. 19.)

A jelentésben kitértek a szovjet flottafejlesztésre is, kihangsúlyozva, hogy ezt is folyamatosan növelik és erősítik. Ezek szerint a Szovjetunió 60 tengeralattjáróval rendelkezik, amelyek közül 30 a legmodernebb típusok közé sorolható, ráadásul várhatóan 1973-ra még további tíz tengeralattjáróval bővül a flotta. A flottafejlesztés eredményeként a szovjetek rendelkeznek a világ legnagyobb halászati flottájával, kereskedelmi flottájukat folyamatosan modernizálják, hadiflottájukat pedig jelentősen megnövelték, és a legújabb fegyverzettel látták el. Fejlesztéseiknek köszönhetően atom-tengeralattjáróik mind fejlettebbek a NATO hasonló egységeinél, amelyekkel képesek lehetnek kereskedelmi hajókat, anyahajókat és rakétahordozó tengeralattjárókat is támadni. A jelentés kiemeli, hogy a Szovjetunió belekezdett egy új nagy hajó, talán anyahajó konstrukciójába is. Ami a szárazföldi haderőt illeti, a Szovjetunió 165, míg a Varsói Szerződés tagállamai további 60 divízióval rendelkeznek, amelyeknek több mint 80%-a a NATO-val határos területen helyezkedik el. Ráadásul folyamatosan fejlesztik szárazföldi haderejüket is, amelyet további T-62-es tankokkal és kétéltű járművekkel erősítenek meg. A jelentés szerint a Varsói Szerződés többi tagállama ugyan nem növelte hadseregének létszámát, de modernizálták felszereltségüket, parancsnokság-szisztémájukat, és ellenőrzésüket.[36] 1974-ben a NATO-tagállamok hírszerző szervei is konferenciát tartottak Brüsszelben, amelyen megerősítették azt a korábbi feltételezést, hogy a Szovjetunió anyahajót épít. Ennek elkészültét 1975-1976 körülre várták, kiemelve, hogy időközben a Fekete-tengeren már egy második anyahajó elkészítésébe is belekezdtek, illetve kihangsúlyozták, hogy 1973-ban a szovjet jelenlét új típusú tankokkal és motorizált gyalogsági egységgel növekedett.[37]

Az 1972. májusi brüsszeli tanácskozáson elhangzottak a Varsói Szerződés és a Szovjetunió haderőfejlesztéseiről és várható támadásáról válaszra késztették a NATO tagállamait. Ennek első lépéseként kijelentették, hogy meg kell akadályozni a nemzeti katonai hozzájárulások csökkentését, a tagállamok hadseregeinek újrastrukturálását a Szövetséggel együttműködve kell végrehajtani,[38] és – a Szovjetunióhoz hasonlóan – nyilvános haderőreformot kell végrehajtani, hogy mind propagandisztikusan, mind pszichológiailag kiegyensúlyozzák a szovjet akciót.[39] A Védelmi Tervező Tanács 1972. december 6-i brüsszeli ülésén a Katonai Tanács elnöke, Steinhoff komoly kritikát fogalmazott meg a tagállamokkal szemben, ismertetve, hogy az azt megelőző 8 évben a tagállamok túl kevés pénzt költöttek a védekezés fejlesztésére, hisz míg a GNP 106%-os növekedést tudott produkálni, addig a védelmi kiadások alig 60%-kal

[36] ILS AGA NATO series [Report on Warsaw Pact] Presentation about the information (Intelligence) concerning Warsaw Pact's military potential, explained at the meeting of NATO Defence Planning Committee, Brüsszel, 1972. május 24. pp. 1-6. https://digitalarchive.wilsoncenter.org/document/145156 (Letöltés ideje: 2022. 04. 19.)

[37] ILS AGA NATO series Report, „NATO conference on Intelligence (AHIWG) for the review of the documents MC 161/73 and 255/73 (Bruxelles, 25th March – 5th april)", Brüsszel, 1974. április 30. pp. 1-9. https://digitalarchive.wilsoncenter.org/document/155227 (Letöltés ideje: 2022. 04. 19.)

[38] ILS AGA NATO series Memorandum by Cheef of Defense Staff, „Political- military considerations with regards to the ministerial meeting of the NATO Defense Planning Committee" (DPC), Brüsszel, 1972. május 24. p. 1. https://digitalarchive.wilsoncenter.org/document/145154 (Letöltés ideje: 2022. 04. 19.)

[39] ILS AGA NATO series General Staff of Defense (SMD) summary report about the meeting of NATO Defense Planning Committee at the ministerial session (Bruxelles, may 24th 1972), Brüsszel, 1972. július 6. p. 4. https://digitalarchive.wilsoncenter.org/document/145155 (Letöltés ideje: 2022. 04. 19.)

növekedtek. Hasonló kritikát fogalmazott meg Luns főtitkár is, míg Laird amerikai védelmi miniszter azzal fenyegette meg európai szövetségeseit, hogy amennyiben az egyes európai országok csökkentik katonai erejüket, abban az esetben az Egyesült Államok csökkenti európai katonai jelenlétét. A fenyegetésre reagálva, Tanassi olasz hadügyminiszter rögtön ki is jelentette, hogy Olaszország kész megemelni katonai hozzájárulásának összegét, sőt, Leber az Eurogroup nevében bejelentette, hogy az európai országok 1972-höz képest a következő évben 1,5 milliárd dollárral többet fognak költeni a védelmi erők fejlesztésére.[40]

A NATO déli szárnyának válsága

Az 1972. decemberi brüsszeli ülésen a jelenlévők aggodalmukat fejezték ki a máltai helyzet kapcsán is. A szigetország 1964. szeptember 21-én kiáltotta ki függetlenségét Nagy-Britanniától, és bár az akkori miniszterelnök, Dr. George Borg kifejezetten jó kapcsolatokat ápolt az Európai Gazdasági Közösséggel (EGK), aminek jeleként 1970-ben Vallettában együttműködési szerződést kötöttek, félő volt, hogy az országban található angol, illetve a NATO-hoz kötődő támaszpontokat ki kell majd üríteni. Ez a félelem felerősödött az 1970-es évek elején, ugyanis 1971 júniusában a kommunista Don Mintoff lett a szigetország miniszterelnöke.[41] A magyar hírszerzéshez eljutott információk szerint az 1960-as években a flottafejlesztés keretein belül a Szovjetunió nem csak Tuniszban és Alexandriában létesített tengeralattjáró-bázist, hanem ajánlatot tett Máltának az ottani brit bázisok átvételére is.[42] Mivel Máltán a NATO számára nélkülözhetetlen bázisok voltak, ezért az Egyesült Államok és Nagy-Britannia félelme erősödött akkor, amikor Don Mintoff még a megválasztása előtt Moszkvában járt. „Von Schiller" szerint az említett két NATO-tagállam attól sem riadna vissza, hogy Don Mintoff megválasztása esetén katonai erőkkel avatkozzon be a szigetország belpolitikai életébe.[43] Erre végül nem került sor, mert a kommunista miniszterelnök némi fizetség fejében megengedte, hogy Nagy-Britannia megtartsa ottani bázisait.[44]

A korban azonban nem csak Máltán adódtak komoly problémái a NATO-nak. Az 1960-as évek végén és az 1970-es évek elején a Szövetség egész déli szárnya válságba került. Spanyolországban, amely bár nem volt tagja a NATO-nak, mégis fontos szerepet töltött be a Földközi-tenger biztonságában az ottani amerikai bázisoknak köszönhetően, az 1960-as évek végéhez közeledve megrendült a polgárháború óta hatalmon lévő Francisco Franco hatalma. Az 1967-ben kiadott az „Állam organikus törvénye" című dokumentum elválasztotta egymástól az állam- és kormányfői pozíciót, és lehetővé tette politikai jellegű társaságok létrehozását, ami elősegítette a politikai pluralizmus kialakulását, igaz, egyelőre még csak a Nemzeti

---

40 ILS AGA NATO series General Staff of Defense (SMD) summary report of the ministerial meeting of the NATO Defense Planning Committee (Bruxelles, december 6th 1972), sent by Minister of Defense Tanassi to Prime Minister Andreotti, Brüsszel, 1973. január 24. p. 1-10. https://digitalarchive.wilsoncenter.org/document/145159 (Letöltés ideje: 2022. 04. 19.)

41 GAMBIN, Kenneth (Szerk.): Malta. Roots of a nation. The development of Malta from an island people to an island nation; Midsea Books Ltd, 2004. pp. 133-134.

42 ÁBTL 3.2.3. Mt 867/1. p. 112. – Információs jelentés, Róma, 1967. augusztus 15.

43 ÁBTL 3.2.3. Mt 867/8. p. 16. – Információs jelentés, Róma, 1971. március 18.

44 GAMBIN i. m. p. 134.

Mozgalmon belül. A jelentkező politikai válság érintette a falangista Mozgalmat is, amelyen belül az „aperturisták", a nyitás hívei egyre hevesebb küzdelmeket folytattak az „inmovilisták"-kal, vagyis a mozdulni nem akarókkal. 1970-től a politikai polarizáció miatt sorra alakultak Spanyolországban az ellenzéki pártok, mint például a szocialista, kommunista, kereszténydemokrata, szociáldemokrata, liberális monarchista, illetve a baszk és katalán nemzeti pártok. Ezzel párhuzamosan az országban diákmozgalmak, munkássztrájkok és nemzetiségi küzdelmek kezdődtek, amelynek során fegyveres akciókat is végrehajtottak. Ezek közül kiemelkedik Carrero Blanco miniszterelnök meggyilkolása, akit az ETA 1973 decemberében autójával együtt felrobbantott. A spanyol politikai bizonytalanságot növelte, hogy a „Caudillo" 1975 novemberében elhunyt, ami után János Károly király engedélyezte a politikai pártok korlátozott működését, majd 1977-ben szabad választásokat rendeztek.[45]

Közben a szomszédos Portugáliában sem alakultak a NATO számára kedvezően az események. Az országot több mint három és fél évtizedig irányító miniszterelnök, Antonio Oliveira Salazar 1968 szeptemberében agyvérzést kapott. Helyét a korábbi kormányaiban miniszteri pozíciót betöltő Marcelo Caetano vette át, aki gondolkodásmódjában, politikai felfogásában szoros rokonságot mutatott Salazarral. Az 1961 óta zajló gyarmati háború miatt azonban a hadsereg alsó- és középtiszti rétegében szervezkedés kezdődött a háború befejezése és a rendszer megdöntése miatt. Az 1973-ban szerveződött Kapitányok Mozgalma végül elérte célját, ugyanis 1974. április 25-én a „szegfűk forradalma" megdöntötte a rendszert.[46] Mivel ezt követően a kommunisták bekerültek a portugál kormányba, ezért az országot kizárták a nukleáris hadászattal kapcsolatos konzultációkból.[47]

Az 1970-es évek elején a Földközi-tenger keleti medencéjében is komoly problémák adódtak. Törökországban 1968 májusában az isztambuli egyetemen sztrájkok és tüntetések kezdődtek, amelyek során a 6. Amerikai flotta tengerészeit is támadás érte. Mivel a Demirel-kormány működésképtelenné vált, ezért 1971. március 12-én a vezérkari főnök átnyújtotta a kormányfőnek a fegyveres erők ultimátumát, amelyben a hadsereg fegyveres hatalomátvételével fenyegette meg a miniszterelnököt. Ennek hatására Demirel lemondott, helyét pedig a hadsereg által kinevezett jogtudós, Nihat Erim vette át. A kormányváltás ellenére azonban az ekkor már évek óta jelen lévő terrorizmus folytatódott az országban. 1971. május 22-én Izrael isztambuli főkonzulját rabolták el és gyilkolták meg, nem sokkal később pedig támadás érte a NATO egyik megfigyelőállomását, amelyben két brit és egy kanadai radartechnikust elraboltak. Később mindhárman életüket vesztették egy tűzharcban. A terrorizmus miatt 11 török tartományban és a nagyvárosokban statáriumot vezettek be, három diákot felakasztottak, és körülbelül 5000 embert, köztük értelmiségieket, írókat, újságírókat, egyetemi tanárokat letartóztattak. 1973-ban végül a hadsereg visszavonult a politikai élettől, és választásokat rendeztek, előtte azonban még módosították az alkotmányt. Az alkotmánymódosításban megszüntették az egyetemek, a tévé és a rádió autonómiáját, korlátozták a polgári szabadságjogokat és a sajtószabadságot, az alkotmánybíróság hatáskörét pedig szűkítették. A választások

---

[45] ANDERLE Ádám: Spanyolország története. Panonica Kiadó, Budapest, 1999. pp. 151-160.

[46] SZILÁGYI István: Portugália a huszadik században; L'Harmattan Kiadó, Budapest, 2015. pp. 80-103.

[47] MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 19.

után hosszas tárgylásokat követően 1974 februárjában megszületett a mérsékelt baloldal és a jobboldal koalíciós kormánya. Ez a koalíciós kormány viszont alig fél év elteltével felbomlott. Új választások kiírása helyett hosszú politikai tárgyalássorozat vette kezdetét, ami után 1975-ben ismét Demirel lett a miniszterelnök.[48] Az országban lévő belpolitikai problémák, a terrorizmus és a nacionalizmus erősödése miatt Törökország kapcsolatai elhidegültek az Egyesült Államokkal és a NATO-val.[49]

Görögországban szintén kiszámíthatatlanná vált a helyzet az 1960-as évek végén, az 1970-es évek elején. A Görög Tisztek Szent Köteléke támogatásával 1967. április 21-én Georgiosz Papadopulosz ezredes néhány alacsonyabb rangú katonatiszttel közösen puccsot hajtott végre. A puccsot követően feloszlatták a parlamentet, felfüggesztették az alkotmányt, és rendkívüli helyzetet vezettek be Görögországban. Másnap, április 22-én II. Konsztantin király törvényesítette Papadopulosz diktatúráját. A hatalomra került katonatisztek tisztogatásba kezdtek a hadseregen belül, internálótáborokat állítottak fel, és bebörtönözték politikai ellenfeleiket, amelynek során görög kommunistákat tartóztattak le, kínoztak meg, és szállítottak a nagyvárosokban felállított gyűjtőhelyekre. A katonai hatalomátvétel azonban nem hozott irányváltást a külpolitikában, Görögország legfontosabb stratégiai partnere továbbra is az Egyesült Államok maradt, és az ország a NATO-tól sem távolodott. A rendszerrel szembeni elégedetlenség növekedése miatt viszont 1973-ban tiltakozások és tüntetések kezdődtek. 1973. november 17-én az athéni műszaki egyetemen zajló tüntetést a hadsereg tankokkal verte szét, ami végül Papadopulosz bukását okozta. Helyét Ioannidisz dandártábornok vette át, aki korábban a katonai rendőrség vezetője volt. Az 1974-es ciprusi válság azonban végleg eltörölte a rendszert. A katonai junta bukása után visszahívták Karamanliszt, Papadopuloszt és Ioannidiszt pedig halálra ítélték, igaz, később az ítéletet életfogytiglani börtönbüntetésre változtatták. Ugyanebben az évben, 1975-ben radikális baloldali diákok létrehozták a November 17-e Csoportot, amely törökellenességén kívül az USA- és NATO-ellenességéről, és különböző terrorcselekmények végrehajtásáról vált ismertté.[50] A katonai junta bukását követően félő volt, hogy Franciaország mintájára Görögország is ki fog lépni a NATO katonai szervezetéből, ami egyet jelentett volna az országban található NATO-támaszpontok felszámolásával.[51]

Törökország és Görögország egymással való kapcsolatát ráadásul jelentősen beárnyékolta Ciprus helyzete. A szigetország függetlenségét 1960. augusztus 15-ről 16-ra virradó éjszaka kiáltották ki, pár hónappal később pedig az ENSZ is felvette tagállamai közé. Az időközben megrendezett elnökválasztáson III. Makariosz jelentős fölénnyel győzött. Makariosz igyekezett a két szuperhatalom versenyéből kimaradni, ezért 1961-ben részt vett az el nem kötelezett országok állam- és kormányfőinek belgrádi értekezletén. Ciprus helyzetét azonban nagyban befolyásolta, hogy területén brit támaszpontok működtek. Az 1959-es zürichi-londoni egyezmények értelmében Nagy-Britannia két szuverén bázist megtarthatott a szigetországban. Több hónapig

---

48 FLESCH István: A Török Köztársaság története; Corvina Kiadó, Budapest, 2007. pp. 88-94.

49 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. p. 19.

50 BALOGH Ádám: Fejezetek Görögország újkori történetéből (A szabadságharctól napjainkig); Magyarországi Görögök Kulturális Egyesülete Csongrád Megyei Helyi Csoport, Szeged, 2013. pp. 108-112.

51 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. p. 19.

tartó, többször is megszakított tárgyalásokat követően végül abban sikerült megállapodni, hogy a Dekelia és az Akrotiri támaszpont méretét is csökkentsék az eredetileg megállapítotthoz képest.[52] A támaszpontok mellett a Kormány Híradó Harcálláspontja (Government Communications Headquarters – GCHQ) lehallgató állomásokat működtetett a szigeten, ráadásul az itt állomásozó 9. ezred alapszintű elemzést is végzett, mielőtt továbbította az adatokat a Központba.[53] A két brit támaszpont és a földrajzi helyzete miatt Ciprus rendkívül fontos volt a NATO számára, ezért a „Von Schiller" által megszerzett információk szerint az Egyesült Államok azt tervezte, hogy felajánlja a szigetországnak a NATO-tagságot, és ha ezt esetleg Makariosz elutasítaná, akkor felvetődött a lehetősége annak, hogy az elnököt eltávolítják Ciprus éléről.[54] Pár évvel később Makariosz ellen rejtélyes merényletet követtek el. 1970. március 8-án a ciprusi elnök helikopterére sortüzet adtak le, de Makariosz sértetlenül szállt ki a gépből. 3 nappal a merénylet után Cipruson letartóztattak 4 embert, akik közül hárman rendőrök voltak. A merénylet napján házkutatást tartottak az elnök korábbi bel- és hadügyminiszterénél, Georgadzisznál, akit bár hivatalosan nem hoztak kapcsolatba a merénylettel, mégis lefoglalták a nála lévő fegyvereket, majd a rendőrség leszállította őt egy Libanonba tartó gépről, és megtiltották, hogy elhagyja Ciprust. Ez után pár nappal ismeretlen tettesek a gépkocsijában agyonlőtték Georgadziszt.[55]

Mindeközben azonban nem sikerült megnyugtatóan rendezni a szigeten élő görögök és törökök sorsát sem. A két etnikum között rendszeresek voltak a gyakran fegyveres összetűzésekbe torkolló konfliktusok, ezért 1963-ban létrehozták a „Zöld vonalat", amely elválasztotta egymástól a görögök és a törökök által lakott területeket. 1974 júliusában viszont a görögországi katonai junta által támogatott ciprusi görög katonatisztek államcsínyt kíséreltek meg azzal a céllal, hogy Makarioszt megbuktassák és a szigetet egyesítsék Görögországgal. Pár nappal később az ott élő törökök védelmére hivatkozva Törökország csapatokat küldött Ciprusra, amelyek megkezdték az ország megszállását. Az 1974 júliusában görög, török és brit részvétellel megrendezett genfi tárgyalásokon végül abban állapodtak meg, hogy a görögök és a ciprusi görög erők elhagyják a töröklakta területeket, és két autonóm adminisztrációt alakítanak ki Cipruson.[56]

Olaszország katonapolitikai helyzete az 1960-as években

Földrajzi helyzetéből adódóan Olaszországnak kettős stratégiai szerepet kellett betöltenie. Mivel mind a kontinentális Európának, mind a mediterrán térségnek szerves részét alkotta, ezért Közép-Európában minden védelmi tudásával segíteni kellett a földközi-tengeri szárny megvédését, míg a mediterrán térségben még összetettebb feladata volt: egyrészt hidat képzett Európa és Afrika között, másrészt

---

52 GÖMÖRI Endre: Makariosz; Kossuth Könyvkiadó, Budapest, 1973. pp. 162-167.

53 PÁL István: A londoni kiküldetés. A Katonai Felderítő Szolgálat Nagy-Britanniában szerzett operatív tapasztalatai a 70-es évek második felében; In: PÁL István – SZÉKELY Gábor (Szerk.): Az Eiffel- torony árnyékában. Majoros István 70 éves; ELTE BTK Új- és Jelenkori Egyetemes Történeti Tanszék, Budapest, 2019. pp. 492- 493.

54 ÁBTL Mt-867/1. p. 118. – Információs jelentés, Róma, 1967. december 27.

55 GÖMÖRI i. m.. p. 240-242.

56 STEPHEN, Michael: The Cyprus question. A concise to the history, politics, and law of the Cyprus Question; Meto Print, London, 2001. pp. 44-46.

Kis-Ázsia irányába a „kinyújtott móló” szerepét töltötte be. Ebből fakadóan részt kellett vennie Közép- és Délnyugat-Európa védelmében, ahol ki kellett egészítenie a görög és török védelmi rendszert, valamint egy esetleges tengeri és légi háború vezetését is magára kellett vállalnia a térségben. Földrajzi helyzete miatt Olaszország két irányból volt kitéve ellenséges támadásnak. Szárazföldön a keleti határai miatt, tengeren és levegőben pedig a Balkán közelsége miatt, ahonnan mind légi-, mind rakétatámadás fenyegette az országot.

Olaszországot a szovjet blokktól két ország választotta el: a semleges, katonailag gyenge Ausztria, és a kommunista vezetés alatt álló, de el nem kötelezett Jugoszlávia. Mivel azonban ezek az országok, ha akartak volna se tudtak volna ellenállni egy szovjet támadásnak, ezért Olaszország igyekezett mindent megtenni védelmi képességeinek növelésére és a NATO megerősítésére. Ennek érdekében engedélyezték IRBM-rakéták telepítését az országba, illetve elfogadták a Szövetség légvédelmi integrációját. Erre már csak azért is szükség lehetett, mivel az 1960-as évekre a Szovjetunió megerősítette katonai kapacitásait Európa és a NATO felé, illetve ezzel párhuzamosan az egész világon bővítette indirekt akcióit, hogy növelni tudja hegemóniáját.

Olaszországnak tehát mind szárazföldön, mind levegőben, mind tengeren erős hadseregre volt szüksége. Míg azonban fegyveres erői közül a haditengerészet megnövelt harcképességgel rendelkezett, addig légi- és a szárazföldi erejét csak mérsékelt harcképességűnek ítélték meg. Ezért 1961-ben az olasz kormány úgy döntött, hogy 70 milliárd lírát költ repülőgépeinek modernizálására, miközben szárazföldi hadseregének fejlesztésére is nagyobb figyelmet fordít az addigiaknál. Ennek elérése érdekében azonban rendkívül fontos volt, hogy az Egyesült Államok elismerje, és anyagilag és fegyveresen is támogassa az olasz célokat.[57]

A szárazföldi haderők megerősítésének fontosságára az Egyesült Államok védelmi minisztere is felhívta a figyelmet. Az Atlanti Tanács miniszteri ülésén Mac Namara hangsúlyozta, hogy problémák vannak a NATO hagyományos erőivel Európa megvédésében, hiszen a Szövetség középső szektorában nincs elég védelmi erő egy a Varsói Szerződés által indított támadással szemben, ezért meg kell erősíteni a Szövetség hagyományos erőit, illetve meg kell egyezni az MLF felállításának kritériumaiban. Beszédében az amerikai védelmi miniszter kifejtette, hogy a SACEUR[58] Parancsnoksága három kategóriába sorolta erőit: harckész állapotban az USA 5 és 2/3, valamint Kanada 1/3 divíziója, magas készültségben Nagy-Britannia 3 és Franciaország 2 divíziója, míg moderált harckészültségben az NSZK 12, Hollandia 2 és Belgium 2 divíziója van. Mac Namara szerint azonban ezek az erők nem lennének elégségesek egy ellenséges támadás megállítására, ezért a Szövetség tagállamainak 5 év alatt 8,5 milliárd dollárt kéne költeniük a hadsereg fejlesztésére. Bár Mac Namara elsősorban a Szövetség középső szektoráról beszélt, hozzátette, hogy a hadi kiadások

[57] ILS AGA NATO series Note assessing Italian Strategic Vulnerability, Brüsszel, 1961. március 8. pp. 2-5. https://digitalarchive.wilsoncenter.org/document/155277 (Letöltés ideje: 2022. 04. 19.)

[58] A SACEUR (Supreme Allied Commander Europe) a Szövetséges Fegyveres Erők Európai Legfelső Parancsnoka. Lásd: Dr. Demeter György (Szerk.): NATO kézikönyv; Stratégiai és Védelmi Kutatóintézet és NATO Információs és Sajtóiroda, Budapest, 1999. p. 290.

20 százalékkal való növelésének szükségessége az északi és déli tagállamokra is igaz.[59]

A hadi kiadások növelése azért is fontos volt Olaszországnak, mert az 1960-as években a NATO tagállamainak többsége az arányos válasz oldalára állt, vagyis egy limitált ellenséges támadás esetére elutasították a stratégiai nukleáris fegyverek bevetését, és az ellenség megbontását a konfliktus kiterjedése nélkül igyekeztek volna elérni. Ez egyet jelentett azzal, hogy hagyományos erők támadása esetén a NATO csak hagyományos erők bevetésével védekezne.[60] A sikeres védekezéshez azonban mindenképpen meg kellett volna erősíteni Olaszország haderejét, ami Andreotti szerint ekkor nem volt erősebb a görög vagy török hadseregnél. Pedig egy erősebb hadsereggel rendelkező erősebb Olaszország nem csak magát lenne képes megvédeni, hanem egyensúlyi szerepet is betölthetne a NATO-n belül.[61] Az európai tagállamok hadseregének erősítésére azért is szükség lett volna, mert Mac Namara bejelentette, hogy az Egyesült Államok ezután csak meghatározott számú amerikai haderőt hajlandó Európában állomásoztatni. Mindezt a racionalizációval indokolta, ami során az Egyesült Államok 3 tényezőt, a stratégiát, az erőt és a gazdasági erőforrásokat igyekezett összhangba hozni katonai kiadásaiban.[62]

Annak ellenére, hogy Olaszország az 1960-as évek elején a szárazföldi haderejének megerősítése mellett döntött, nincs nyoma annak, hogy az évtizedben ebben jelentős fejlődést tudtak volna elérni. A szovjet flottafejlesztés miatt azonban a NATO belekezdett földközi-tengeri flottájának megerősítésébe, ami Olaszországot is érintette. 1964-ben döntés született az MLF tengeri egységeinek elhelyezésére a Mediterráneumban. Bár Görögország és Törökország is felkészült arra, hogy az egységek számára a területükön létesítenek bázist, az ezzel foglalkozó Munkacsoport elsődleges céljai között Szardínia, Szicília, vagy Málta szerepelt, igaz, Olaszország egyelőre még nem foglalt pozíciót abban a kérdésben, hogy engedélyezné-e területén bázis kiépítését, vagy csatlakozik-e egyáltalán az MLF-hez. Az olasz kormány ragaszkodott ahhoz, hogy amennyiben a csatlakozás mellett döntenek, abban az esetben mindenképpen meg kell állapítani egy financiális határt. A csatlakozás 25 hajó esetén évi kb. 20 milliárd líra kiadást jelentene Olaszország számára, ami tekintve az olasz gazdaság helyzetét, tarthatatlannak bizonyult. Az ország vezetése reálisabbnak látta azt, hogy 10 vagy 12 hajóval csatlakozna az egységhez, ennek összegét ugyanis még képesek lettek volna kigazdálkodni.[63]

---

[59] ILS AGA NATO series Report by Permanent Representation to NATO Alessandrini to Minister of Defense Andreotti, Brüsszel, 1963. január 3. pp. 2-6. https://digitalarchive.wilsoncenter.org/document/155295 (Letöltés ideje: 2022. 04. 19.)

[60] ILS AGA NATO series Message by Ministry of Foreign Affairs, Directorate General for Political Affairs and Security (DGAP), „NATO strategy", Brüsszel, 1963. december 4. pp. 3-5. https://digitalarchive.wilsoncenter.org/document/155301 (Letöltés ideje: 2022. 04. 19.)

[61] ILS AGA NATO series Report, „Point 2. NATO situation", Brüsszel, 1963. p. 16. https://digitalarchive.wilsoncenter.org/document/155294 (Letöltés ideje: 2022. 04. 19.)

[62] ILS AGA NATO series Memorandum by Ministry of Defense, „NATO strategy", Brüsszel, 1963. december 10. p. 3. https://digitalarchive.wilsoncenter.org/document/155300 (Letöltés ideje: 2022. 04. 19.)

[63] ILS AGA NATO series Memorandum by Ministry of Foreign Affairs, „Multilateral Nuclear Force", Brüsszel, 1964. pp. 6-8. https://digitalarchive.wilsoncenter.org/document/155307 (Letöltés ideje: 2022. 04. 19.)

A NATO Katonai Tanácsának ugyanebben az évben megrendezett ülésén szóba került a Déli Szektor Parancsnokságának átszervezése, amit viszont egyelőre Nagy-Britannia megvétózott Málta kérdéses jövőjére hivatkozva.[64] Az átszervezés így az évtized második felére maradt, amelynek keretein belül az Egyesült Államok rakétakilövő hajók átadásával, illetve Lampedusán és Pantellerián tengeri és légi támaszpont kiépítésével igyekezett megerősíteni az olasz haditengerészetet.[65] Az átszervezésbe beletartozott egy új egység felállítása a Földközi-tengeren Maritime Air Force Mediterranean (MarAirMed) néven, amelynek támaszpontjait Nápolyban, Szicílián, Milánóban, Tarantóban, Máltán és Cipruson tervezték elhelyezni.[66] Az amerikai, angol és olasz vegyes flottából álló egység felállítása azonban akadozott és nem az előzetesen elvártak szerint fejlődött, ugyanis hiányoztak hozzá az angol és az olasz egységek.[67]

A MarAirMed felállításával kapcsolatos problémák ellenére az 1960-as évek végén alkalmazkodva a nemzetközi helyzet változásaihoz és a gazdasági fejlődés nyújtotta lehetőségekhez, a NATO folytatta az át-, illetve újjászervezést, amelynek keretein belül Dél-Európa védelmének egységesítése érdekében megszüntették az eddigi mediterrán főparancsnokságot (Commander in Chief of Allied Forces Mediterranean – CINCAFMED), aminek szerepét a Dél-Európai Tengerészeti Parancsnokság (Commander of Naval Forces Southern Europe – COMNAVSOUTH) vette át.[68] Ezzel párhuzamosan egy új készenléti haditengerészeti egységet is felállítottak a Földközi-tengeren NAVOCFORMED (Naval On-Call Force Mediterranean) néven. Ennek az új készenléti egységnek a parancsnoka egy olasz tiszt lett, ami jelezte Olaszország szerepének növekedését a Szövetségen belül.[69]

Olaszország helyzetének változása a NATO-n belül

Olaszország helyzete a NATO-n belül sokat változott az 1960-as években. Az évtized első felében még nem játszott jelentős szerepet a Szövetségben, amit bizonyít, hogy 1963-ban az olasz kormány hiába szerette volna elérni, hogy a Katonai Tanács elnökének egy olasz jelöltet válasszanak meg. A megválasztás érdekében az olasz képviselők egyeztetéseket folytattak a brit, a német és a francia kormány küldötteivel, de ezektől tartózkodó válaszokat kaptak. Az olasz követ úgy vélte, hogy az NSZK inkább a belga jelöltet fogja támogatni, és ebben mellé áll majd Nagy-Britannia és az Egyesült Államok is, aminek az az oka, hogy Olaszország jövőjével kapcsolatban nem túlságosan optimisták a NATO-ban. A követ szerint az olasz jelöltséget egyedül Törökország és Görögország támogatná, ezeknek az államoknak azonban nincs döntő

---

64 ILS AGA NATO series Memorandum by Chief of Defense Staff Aldo Ross to Minister of Defense, „32nd Meeting of the Military Committee – SHAPEX 64 – conversation with General Taylor"; Brüsszel, 1964. június 16. p. 3. https://digitalarchive.wilsoncenter.org/document/155302 (Letöltés ideje: 2022. 04. 19.)

65 ÁBTL 3.2.3 Mt-867/1. p. 118. – Információs jelentés, Róma, 1967. augusztus 15.

66 A hírszerzés jelentéseiben az egység rövidítése tévesen MARAIMED-ként szerepel. Lásd: ÁBTL 3.2.3 Mt-867/2. p. 109. – Információs jelentés, Róma, 1968. november 26.

67 ÁBTL 3.2.3 Mt-867/3. p. 22. – Információs jelentés, Róma, 1969. november 5.

68 ILS AGA NATO series Report, „Legitimacy, situation and prospects of the Atlantic Alliance", Brüsszel, 1969. pp. 5-6. https://digitalarchive.wilsoncenter.org/document/165234 (Letöltés ideje: 2022. 04. 19.)

69 MINOLFI i. m. p. 105.

szavuk a Szövetségen belül.[70] Míg tehát az évtized első felében az olasz jelöltek általában nem élvezték a nagyobb tagállamok támogatását, addig az évtized végén nem csak a NAVOCFORMED, hanem a COMNAVSOUTH, és a Nemzetközi Integrált Fővezérség igazgatója is egy olasz admirális illetve tábornok lett.[71]

Olaszország NATO-n belüli szerepének változását egy 1970-es hírszerzési jelentés is megerősíti. A jelentés szerint az Egyesült Államok a következő években kiemelt szerepet szán Olaszországnak, ennek érdekében pedig igyekszik megerősíteni gazdasági és politikai ellenőrzését az ország felett, hogy ezáltal erősítse az amerikai katonai és politikai pozíciókat az országban.[72] Az Egyesült Államok pozícióinak olaszországi erősítése és Olaszország földközi-tengeri szerepének növelése összefüggésben állhatott azzal az amerikai tervvel, miszerint az amerikai 6. flotta bizonyos alakulatait és hajóit kivonnák a Mediterrán térségből, hogy azokat a vietnami háborúban tudják bevetni[73], az amerikai fegyveres erők áthelyezésének ellensúlyozására pedig új olasz tengeri és légi egységeket állítanának fel a Földközi-tengeren.[74] Ezzel párhuzamosan szóba került, hogy amerikai segítséggel, de az Egyesült Államok részvétele nélkül új hajóegység hoznának létre a NATO számára is, mivel ebben az időszakban az USA célja mind az amerikai, mind a szovjet erők Földközi-tengerről történő kivonása volt, aminek védelmét így Nagy-Britannia, Franciaország, Spanyolország, Törökország és Olaszország venné át.[75] A Földközi-tengerről történő esetleges csapatkivonások voltak az egyik fő témái a szovjet külügyminiszter 1970. november 10-13-i római látogatásának. Gromiko azonban meglehetősen merev álláspontot képviselt a kérdésben, és az esetleges haditengerészeti erők csökkentéséről szóló olasz felvetésre azzal reagált, hogy először katonai vizsgálatokat kellene elvégezni, és csak utána lehetne tárgyalni az esetleges kivonásról.[76]

Olaszország katonapolitikai helyzete az 1970-es években

Mivel az 1960-as években elmaradt az olasz szárazföldi haderő fejlesztése, ezért az 1970-es évek elején az olasz kormány úgy döntött, hogy fokozott figyelmet fog fordítani erre. Emiatt megemelték a szárazföldi haderő fejlesztésre fordítandó katonai költségvetést, míg a légierő és a haditengerészet kapcsán az a határozat született, hogy változatlan költségvetésből fog gazdálkodni, de erőteljesebben kell alkalmazkodnia a

---

70 ILS AGA NATO series Report by Ambassador Quaroni to Minister of Foreign Affairs Piccioni, „General de Martino's candidacy and Standing Group", Brüsszel, 1963. július 9. pp. 1-5. https://digitalarchive.wilsoncenter.org/document/155297 (Letöltés ideje: 2022. 04. 19.)

71 ILS AGA NATO series Report, „Legitimacy, situation and prospects of the Atlantic Alliance", Brüsszel, 1969. p. 7. https://digitalarchive.wilsoncenter.org/document/165234 (Letöltés ideje: 2022. 04. 19.)

72 ÁBTL 3.2.3. Mt-867/6. p. 116. – Információs jelentés, Róma, 1970. szeptember 10.

73 Vietnamban az 1964-es tonkini incidensre hivatkozva -amikor felrobbant egy amerikai hadihajó- az amerikai kormány egyre nagyobb erőket vetett be, miközben folyamatosan bombázta Észak-Vietnamot. Lásd: BALOGH András: Bevezetés Délkelet-Ázsia történelmébe; ELTE Eötvös Kiadó, Budapest, 2015. p. 371.

74 ÁBTL 3.2.3. Mt-867/7. p. 71. – Információs jelentés, Róma, 1970. december 11.

75 ÁBTL 3.2.3. Mt-867/7. p. 14. – Információs jelentés, Róma, 1970. október 23.

76 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1970/69. doboz – Jelentés, Róma, 1970. december 2. p. 1.

NATO specializációs követeléseihez. Azért hozták ezt a döntést Rómában, mert az olasz katonai és politikai vezetés elsőrendű feladatként határozta meg az északkeleti határ biztosítását, az olasz hadműveleti koncepció fő irányaként pedig a szocialista közösséget, elsősorban Jugoszláviát jelölték meg.[77] Ezt alátámasztja egy 1971-es olasz katonapolitikai jelentés, amelyből kiderül, hogy az ország szárazföldi hadseregének nagy része, egészen pontosan a III., IV., V. és VI. Hadtest is a keleti határ közelében és a Pó-síkságon helyezkedik el, ami azt jelentette, hogy ebben a térségben állomásozott 2 páncélos divízió, 2 gyalogos divízió, további 2 gyalogos egység és az alpesi hadosztályok is, miközben Olaszország középső és déli területeire mindössze 1-1 gyalogos hadosztály jut. A jelentés kiemeli, hogy ez a diszharmonikus elhelyezkedés azért is jelent problémát, mert a hadsereg részt vesz a természeti katasztrófák (földrengések, árvizek) kezelésében, és közben közbiztonsági feladatokat is ellát. A jelentés szerint a fegyveres erőknek azonnali reformra lenne szükségük, amelynek magában kell foglalnia az átstrukturálást, illetve a szárazföldi haderő mechanizálását, és a katonák mozgatásához modern eszközöket kell alkalmazni. Ennek során helikopteres egységeket kell felállítani, mert a vietnámi tapasztalatok azt mutatják, hogy ezek nem csak megkönnyítik a katonák gyors mozgatását, hanem alkalmasak gerilla-hadviselés ellen is, amikkel a jelentés szerint Európában és Olaszországban is számolni kell a kommunisták részéről.[78]

Bár a katonapolitikai jelentés nem tér ki rá, de Olaszországban jelentős külföldi erők is állomásoztak. Az 1970-es évek elején például a brit haderő többek között két szakasszal, illetve Phantom, Buccaneer és Camberra típusú repülőgépekkel is jelen volt elsősorban az ország északi részén és Szardínia szigetén.[79]

Ezzel párhuzamosan Tanassi honvédelmi miniszter kijelentette, hogy Olaszországra és fegyveres erőire híd szerep hárul, ami miatt kettős szerepet kell betöltenie. Egyrészt teljesítenie kell a NATO által meghatározott feladatait, másrészt létre kell hoznia egy bármelyik fronton beavatkozásra képes haderőt, amely akkor is meg tudja védeni az országot, ha a szövetségesek nem működnek együtt. Kijelentését azzal indokolta, hogy *„csökkent ugyan egy általános háború valószínűsége, ha állandó is a veszély a Varsói Szerződés erejének növekedése miatt. Nőtt viszont a Földközi-tenger felől jövő fenyegetés, valamint az olyan helyi válságok lehetősége, amelyek az olasz területeket is érinthetik. Állandóan számolni kell egy esetleges, a jugoszláv politikai viszonyok hirtelen változásából következő válsággal."*[80]

Az olasz szárazföldi hadsereg megerősítésének szükségességét szintén alátámasztotta egy 1974-es brüsszeli NATO hírszerzési konferencia, melyen a SID munkacsoportja is részt vett. A konferencián elhangzott, hogy a Varsói Szerződés kezdetben valószínűleg hagyományos erőkkel támadna, ez azonban gyorsan átalakulhatna nukleáris támadássá. A konferencián kihangsúlyozták, hogy Olaszországot 14 divízió fenyegeti, amiből 6 magyar, 4 Magyarországon állomásozó

---

77 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 17.

78 ÁBTL 3.2.3. Mt-867/8. p. 131/128-130. AIPE-jelentés

79 National Archives (NA) Ministry of Defence, Chiefs of Staff Committee, 1973. január 23. pp. 217-245. https://www.nationalarchives.gov.uk/ (Letöltés ideje: 2022. 06. 14.)

80 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1972/82. doboz – Jelentés, Róma, 1972. január 20. p. 3.

szovjet és további 4 szovjet stratégiai tartalék.[81] Mivel Olaszország Magyarországot kapta kiemelt viszonylatként, és mivel Magyarország felől számítottak egy esetleges szovjet és magyar katonai beavatkozással, ezért az ország nem is vett részt az ekkor zajló fegyverzetcsökkentési tárgyalásokban.[82] Az MBFR-konferenciát[83] az olasz vezérkar amúgy is ellenezte, mert véleménye szerint a tárgyalásokat megfelelő előkészületek nélkül kezdték meg, és ezeket csak a helsinki konferencia után kéne lefolytatni.[84]

Az 1970-es évek elején a portugál forradalom, a ciprusi válság, az olajválság és az újabb arab-izraeli háború[85] következtében megnőtt az esélye a politikai egyensúly felborulásának a Földközi-tengeren.[86] A bizonytalan hadászati helyzet szűkítette az Egyesült Államok manőverezési lehetőségeit a térségben, ami jelentősen befolyásolta Olaszország katonapolitikai helyzetét, ezért az olasz kormány differenciáltabb politikába kezdett a Közel-Keleten, ezzel megpróbálva elérni, hogy Nyugat-Európa közvetítője legyen az arab országok felé.[87] A differenciáltabb politikára Andreotti már 1972-es miniszterelnöki beszédében utalt. A beszédben Andreotti – amellett, hogy felhívta a figyelmet a NATO-n belüli katonai erőfeszítések fokozásának szükségességére, ami miatt az olasz kormány tárgyalásokba kezdett az angol és a francia vezérkarral a felszerelések szabványosításáról – kijelentette, hogy Olaszország fokozott diplomáciai tevékenységbe kezd a Földközi-tengeren, mivel célja egy a helsinki konferenciához hasonló földközi-tengeri konferencia összehívása.[88]

A fokozott diplomáciai tevékenység főleg azután lett nélkülözhetetlen, hogy Görögország bejelentette kiválási szándékát a NATO-ból. Ennek következtében szükségessé vált a Szövetség hadműveleti terveinek átdolgozása, új haditengerészeti és légitámaszpontok, illetve atomraktárak létesítése, hiszen innentől kezdve a NATO csak az amerikai 6. flottára, a brit támaszpontokra és Olaszországra számíthatott a

---

81 ILS AGA NATO series Report, „NATO conference on Intelligence (AHIWG) for the review of the documents MC 161/73 and 255/73 (Bruxelles, 25th March- 5th April)", Brüsszel, 1974. április 30. pp. 1-4. https://digitalarchive.wilsoncenter.org/document/155227 (Letöltés ideje: 2022. 04. 19.)

82 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1972/82. doboz – Jelentés, Róma, 1972. január 20. p. 5.

83 Az MBFR-tárgyalásokat (Mutual and Balanced Force Redactions – Kölcsönös és kiegyensúlyozott haderőcsökkentés) 1973. október 30-án nyitották meg hivatalosan Bécsben a NATO és a Varsói Szerződés tagállamainak részvételével. A tárgyalások célja az NDK, az NSZK, a Benelux-államok, Csehszlovákia és Lengyelország területén felvonultatott hagyományos védelmi és támadó erők kölcsönös csökkentése volt. Lásd: HORVÁTH – PARAGI – CSICSMANN i. m. pp. 215-216.

84 ÁBTL 3.2.3. Mt-867/11. p. 61. – Információs jelentés, Róma, 1973. április 9.

85 A háború 1973. október 6-án Egyiptom Izrael elleni támadásával kezdődött. A Jom Kippur ünnepére időzített támadás váratlanul érte Izraelt, mely Szíria egyidejű támadása miatt történelmének legkritikusabb napjait élte át. A háborúnak végül az ENSZ-tárgyalások és a „kék sisakosok" megérkezése vetett véget. Lásd: FISCHER i. m. p. 291.

86 MINOLFI i. m. p. 105.

87 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében. A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 18.

88 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1972/82. doboz – Jelentés, Róma, 1972. június 29. p. 1.

Földközi-tengeren, ami nem csak a térségben, hanem a Szövetségen belül is növelte Róma hadászati-hadműveleti szerepét. Bár 1974-ben még nem vált véglegessé Görögország kiválása, az olasz kormány már bekapcsolódott a földközi-tengeri stratégia átértékelésével foglalkozó NATO-tevékenységbe, hiszen az esetleges kiválás következtében Szicíliára nagyobb szerep hárulna, és a görögországi támaszpontokat áthelyeznék Olaszországba. Mivel azonban a támaszpontok áthelyezését a PCI és a PSI hevesen ellenezte, ezért a belpolitikai helyzet megint csak akadályozta az olasz katonai vezetés szándékait. A probléma megoldása érdekében az olasz kormány hármas célt hirdetett: a közvélemény előtt igyekezett megőrizni a nemzeti függetlenség látszatát, fenntartotta az Egyesült Államok iránti elkötelezettségét és erőfeszítéseket tett a NATO déli szárnya egységének helyreállítására.

A déli szárny egységének helyreállítása érdekében Olaszország igyekezett közvetíteni Görögország és az Egyesült Államok között. Az olasz honvédelmi miniszter, Andreotti a görög, míg Leone köztársasági elnök az amerikai vezetéssel tárgyalt. Andreotti azt mondta görög kollégájának, hogy mivel Olaszország nem alkalmas a görögországi amerikai és NATO-támaszpontok fogadására, ezért Róma kész anyagi segítséget nyújtani a görög kormánynak azért, hogy a bázisok maradhassanak.[89] Közben Leone washingtoni látogatásán Ford elnök bejelentette, hogy az Egyesült Államok kész 5-7 milliárd dollárral támogatni új olaszországi támaszpontok felállítását, de csak abban az esetben, ha Róma teljesíti két feltételét. Az egyik a történelmi kompromisszum kizárása volt, a másik, hogy Olaszország vállaljon nagyobb kötelezettséget a NATO-ban. Ez utóbbi feltétel miatt viszont az olasz vezetés kénytelen volt módosítani katonapolitikai prioritásait, hiszen így az észak-keleti határa mellett a Földközi-tengerre is nagyobb figyelmet kellett fordítania, ami módosulást jelentett a haderőnemek szempontjából, mert a szárazföldi haderő fejlesztésével párhuzamosan fejlesztenie kellett haditengerészetét és légierőjét.[90]

A magyar hírszerzés információi szerint az 1970-es évek elején Olaszország belekezdett a haditengerészet és légierő fejlesztésébe. A Pentagon kutatási igazgatója, Foster javaslatot tett az NSZK-nak, Nagy-Britanniának, Franciaországnak és Olaszországnak új rakéták fejlesztésére, aminek során az olasz haderő tenger-tenger rakétákkal, repülőgépekkel és tengeralattjárókkal erősödne. Ezen kívül az Egyesült Államok felajánlotta Romának lövegek és rakéták közös gyártását is.[91] Ha a magyar hírszerzés információi pontosak voltak, akkor ez a közös fejlesztés gyorsan kezdetét vette, hiszen már 1972 decemberében arról szólt az egyik információs jelentés, hogy az olasz hadiipar fellendülő szakaszban van, és az amerikai haditengerészettel közösen új gépágyú és új felszín-felszín rakéta fejlesztésébe kezdtek Olaszországban.[92]

Az olasz vezetés számára a szárazföldi haderő fejlesztése szintén sürgős lett volna, hiszen az 1970-es évek elején az olasz katonapolitika kettős célkitűzést jelölt

---

89 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Jelentés, Róma, 1974. szeptember 30. p. 1.

90 MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében. A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 18-24.

91 ÁBTL 3.2.3. Mt-867/10. p. 206. – Feljegyzés, Budapest, 1972. július 5.

92 ÁBTL 3.2.3. Mt-867/11. p. 34. – Információs jelentés, Budapest, 1972. december 15.

meg. Egyrészt védeni kívánta az ország észak-keleti határszakaszát, másrészt a szocialista országok, elsősorban Magyarország ellen biztosítania kellett volna a NATO közép- és dél-európai hadszíntere közötti kapcsolatot. Ennek érdekében az olasz katonapolitika az 1970-es években Ausztriára és Jugoszláviára összpontosított.[93] Ezzel a két országgal viszont területi viták miatt Olaszországnak nem voltak jók a kapcsolatai.

Az olasz–osztrák és az olasz–jugoszláv viszony

Olaszország és Ausztria viszonyát Alto-Adige (más néven Dél-Tirol) kérdése árnyékolta be. A terület az első világháborút követően került Olaszországhoz. A második világháború után, 1946. szeptember 5-én a két ország egyezményt írt alá, amely garantálta az itt élő német nemzeti kisebbség jogainak védelmét. Az egyezmény értelmében elismerték a német nyelv egyenjogú használatát a közigazgatásban, engedélyezték az anyanyelvi oktatást az alsó- és középiskolákban, valamint arányos részvételi jogot biztosítottak a közalkalmazottak körében. Ezen kívül a német nyelvű lakosság teljes egyenjogúságot élvezett az olasz nyelvű lakossággal, megőrizhette etnikai jellegét, biztosították számára a gazdasági és kulturális fejlődést, illetve az itt élő németek autonóm regionális törvényhozó és végrehajtó szerveket létesíthettek.[94] Az egyezményben biztosított jogok ellenére Alto-Adige helyzete a későbbiekben is feszültséget eredményezett Olaszország és Ausztria között, ugyanis terrorista csoportok rendszeresen hajtottak végre merényleteket a területen. A terrorista merényletek közül az 1966-ban végrehajtott akciók kapták a legnagyobb figyelmet, amelyek során augusztus 25-én két pénzügyőr, szeptember 9-én pedig két határőr vesztette életét.[95]

Az olasz és az osztrák kormány végül 1969 novemberében megállapodást írt Alto-Adige autonómiájáról, amely rendezte a terület kérdését, és lehetőséget adott a két ország közötti katonapolitikai kapcsolatok kiszélesítésének. Elsőként 1970 őszén a 4. olasz alpesi hadtest törzsfőnöke találkozott a 6. osztrák vadászdandár parancsnokával, nem sokkal később pedig megkezdődtek a magasabb szintű megbeszélések is. 1971 júniusában az osztrák vezérkari akadémia parancsnoka utazott Olaszországba, hogy tárgyalásokat folytasson Mereu olasz vezérkari főnökkel. A látogatást még ugyanezen év őszén Mereu viszonozta. Néhány évvel később, 1973 áprilisában az olasz védelmi miniszter, Tanassi utazott Bécsbe, hogy tárgyalásokat folytasson az osztrák kormány tagjaival. A tárgyalások során Olaszország teljesítette a NATO megbízását, miszerint Ausztrián keresztül kell összeköttetést biztosítania az NSZK-ban állomásozó szövetséges erőkkel.[96]

---

[93] MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 25.

[94] FÖLDESI Margit – STELLA Szonja: Egy másik vesztes; Olaszország 1943-1947. Kairosz Kiadó, Budapest, 2006. p. 196.

[95] MAMMARELLA, Giuseppe: L'Italia contemporanea (1943- 2011); Società editrice il Mulino, Bologna, 2012. p. 301.

[96] MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében. A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. pp. 26-28.

Olaszországnak az Ausztriával fennálló kapcsolatánál azonban bonyolultabb volt a Jugoszláviához fűződő viszonya. A két ország között Trieszt kérdése okozott feszültséget, amelyet évtizedeken keresztül nem tudtak megoldani. A terület 1943. szeptember 8-án német csapatok megszállása alá került, és szeptember 23-án a Mussolini által vezetett Olasz Szociális Köztársasághoz csatolták. Közben viszont Tito is bejelentette igényét Triesztre és környékére. A második világháború végéhez közeledve, 1945. május 1-jén a jugoszláv hadsereg elfoglalta a várost, és június 12-ig megszállása alatt tartotta, bevezetve a jugoszláv közigazgatást. Ezt követően Trieszt a Szövetséges Katonai Kormány hatáskörébe került. Az 1947-es párizsi béke kettéosztotta a területet, az A-övezet angolszász fennhatóságba, míg a B-övezet jugoszláv irányítás alá került. Az 1954. október 6-i londoni memorandum értelmében az A-övezet olasz fennhatóság alá került, pár héttel később közigazgatását át is adták Romának. Trieszt kérdését azonban csak az 1970-es évek közepén sikerült megnyugtatóan rendezni. Az 1975. november 10-én Olaszország és Jugoszlávia által megkötött osimói szerződés az A-övezetet végérvényesen Olaszországhoz csatolta.[97]

Változások az olasz katonapolitikában

Az 1970-es évek elején az olasz fegyveres erőkben egy új nemzedék kezdett feltűnni, ami az ország katonapolitikájának megváltozásához vezetett. Ez az új nemzedék új felfogást, új mentalitást hozott, aminek lényege egy technokratikus, a korábbinál hatékonyabb védelmi hozzáállás volt, ami egyet jelentett mind a haderő, mind az operatív doktrinák újrastrukturálásával. Erre az újrastrukturálásra már 1972-ben Henke admirális, a vezérkar főnöke utalt, amikor kijelentette, hogy *„a nemzeti védelmi erőknek képesnek kell lenniük önállóan beavatkozni olyan fenyegetésekkel szemben, amelyek esetében nem lehet biztonsággal támaszkodni a szövetséges nemzetek közvetlen és azonnali együttműködésére”*. Ez az új mentalitás megjelent a haditengerészet 1974-es Fehér Könyvében is, amelyben a biztonságról egy új, autonóm felfogást fogalmaztak meg. A Fehér Könyv szerint Olaszországnak új beavatkozási egységeket kell felállítania, amelyek nem csak a Kelet-Nyugat konfliktusában, hanem kisebb konfliktusokban és helyi problémák kezelésében is bevethetők. Ezek az új egységek nem veszélyeztetnék a NATO erőinek katonai integrációját, hanem autonóm funkciókat töltenének be az olasz érdekeltségű területeken, mint például a Mediterrán térség vagy a Közel-Kelet, és képesek lennének preventív szerepet is betölteni. Ehhez azonban mindenképpen szükséges az olasz haderő modernizációja és újrastrukturálása.[98]

Mivel az 1960-as és 1970-es években Olaszország nem lett volna képes megvédeni magát egy esetleges, a Varsói Szerződés tagállamai részéről érkező ellenséges támadástól, ezért Róma szerette volna fejleszteni nukleáris képességeit. Ezzel kapcsolatban Saragat köztársasági elnök úgy nyilatkozott a ‘60-as években, hogy *„Mi olaszok inkább iskolákat, kórházakat és házakat építünk [...] de azt akarjuk, hogy Olaszország képes legyen gyorsan atombombát gyártani.”*[99] Ebben az évtizedben azonban már megkezdődtek az első tárgyalások a stratégiai nukleáris fegyverek ellenőrzéséről, csökkentéséről, amelyeken a legsürgetőbb megoldásra váró

[97] FÖLDESI – STELLA i. m. pp. 136-138.
[98] MINOLFI i. m. p. 107.
[99] MAMMARELLA – CACACE i. m. p. 223.

probléma a nukleáris fegyverrel rendelkező országok lehetséges megsokszorozódásának megakadályozása volt.[100] Hosszas tárgyalásokat követően 1968 júliusában alá is írták az atomsorompó-szerződést (Treaty on the Non-Proliferation of Nuclear Weapons – NNPT), mely 1970-ben lépett hatályba. A szerződés 3 pilléren nyugodott: a katonai célra használható nukleáris technológiák terjedésének megakadályozása, a nemzetközi felügyelet melletti leszerelés, és az atomenergia békés célú felhasználása.[101] Bár a tárgyalásokon Olaszország aktívan részt vett, vonakodott a szerződés aláírásától. Ezt végül csak az Atlanti Szövetség nyomására volt hajlandó megtenni 1970-ben, de a parlamenti viták miatt a ratifikálás elmaradt. Ezzel párhuzamosan a magyar hírszerzés információi szerint 1968-ban Nedici olasz külügyminiszter azzal a kéréssel fordult az USA-hoz, hogy a NATO-n belül a tagállamok kapjanak nagyobb szabadságot a nukleáris fegyverekkel való rendelkezésben, miközben Amerikában azt feltételezték, hogy Olaszország már rendelkezik atomfegyver-prototípussal.[102] Ezt az információt egy 1974-es nagykövetségi jelentés is megerősíti, amely szerint Olaszország valószínűleg először 1966-ban jutott el odáig, hogy képes lett volna atomszerkezetet robbantani, amit akkor Saragat meg is erősített.[103] Néhány hónappal később a nagykövetség azt írta, hogy Róma az Egyesült Államok sürgetése ellenére sem fogja ratifikálni az atomsorompó-szerződést, aminek az oka, hogy Olaszország képes atomfegyver gyártására.[104]

Összegzés

Az MBFR-tárgyalások és a SALT-szerződés[105] megkötése kedvező feltételeket biztosítottak egy összeurópai biztonsági értekezlet összehívásának, amelynek szükségességét már egy 1966-os bukaresti és 1969-es budapesti felhívás is sürgetett. Hosszas előkészítést követően végül 1973. július 3-án Helsinkiben 33 európai és 2 amerikai ország jelenlétében megnyitották az Európai Biztonsági és Együttműködési Értekezletet (EBEÉ). A július 3-7-ig tartó nyitó szakaszon a jelenlévők kifejtették elképzeléseiket az európai biztonság modelljéről, majd az 1973. szeptember 10-től 1975. július 21-ig Genfben megrendezett második szakaszban a 35 állam közötti kapcsolatok irányító elveiről és előírásairól állapodtak meg. Az EBEÉ ünnepélyes zárószakaszára megint csak a finn fővárosban került sor 1975. július 31. és augusztus 1. között. A záróokmány első kosarába biztonságpolitikai és katonai aspektusok kerültek, a második kosár a gazdasági, technikai, környezetvédelmi együttműködésről, míg a harmadik kosár a humanitárius területekről, emberi jogokról, és a mediterrán térségben való együttműködésről szólt. Bár a konferenciát

---

[100] SILVESTRI, Stefano: Il dibattito sulla non-proliferazione nucleare; In: MERLINI, Cesare (Szerk.): La politica estera dell'Italia. Cinquant'anni dell'Istituto Affari Internazionali; Società editrice il Mulino, Bologna, 2016. p. 72.

[101] HORVÁTH – PARAGI – CSICSMANN i. m. p. 188.

[102] ÁBTL 3.2.3 Mt-867/2. p. 87. – Információs jelentés, 1968. szeptember 3.

[103] MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Jelentés, Róma, 1974. október 11. p. 1-2.

[104] MNL OL XIX-J-1-j Olaszország KÜM TÜK 1975/108. doboz – Jelentés, Róma, 1975. január 27. p. 5.

[105] A SALT I. (Strategic Arms Limitation Talks) szerződést 1972. május 26-án írták alá Moszkvában. A szerződés rögzítette a szárazföldről indítható ICBM és a tengeralattjáróról indítható SLBM (Submarine Launched Ballistic Missiles) felső számát, ezen kívül tiltotta szárazföldi rakétaindító állomások építését, és szabályozta a támadórakéták korszerűsítésének módozatait. Lásd: HORVÁTH – PARAGI – CSICSMANN i. m., p. 213.

még számos utókonferencia követte, a helsinki értekezletet tekinthetjük a hidegháborús enyhülés csúcspontjának.[106]

Az értekezletet megelőző bő egy évtizedben a NATO-nak, és azon belül Olaszországnak komoly problémákkal kellett szembenéznie. A Szovjetunió előretörése, a szovjet flotta folyamatos térnyerése és erősítése, a Varsói Szerződés és a Szovjetunió szárazföldi és légi erőinek fejlesztése arra ösztönözte a Szövetséget, hogy megerősítse saját védelmi képességeit. Mindeközben Franciaország kilépése a katonai szervezetből, a déli szárny államaiban lezajlott forradalmak, Málta és Ciprus kérdése, illetve a vietnami háború és a közel-keleti arab-izraeli konfliktusok miatt az 1960-as és az 1970-es években a NATO-t át kellett szervezni. Ezzel párhuzamosan Olaszországban is gondok voltak. A gazdaság instabil helyzete, az állandó kormányválságok, a kommunista párt egyre népszerűbbé válása, az államcsíny-kísérletek és a terrorcselekmények rendkívül ingataggá tették Róma helyzetét a Szövetségen belül.

Ennek ellenére a Kereszténydemokrata Párt végig megőrizte vezető szerepét, a párt meghatározó politikusaiból lettek miniszterelnökök, és a kommunistákat sikerült távol tartani a kormánytól, nem úgy, mint Portugáliában. Ezen kívül, bár államcsíny-kísérletek és terrorcselekmények gyengítették az országot, mégis sikerült elkerülni a belpolitikai status quo radikális megváltozását, amit sem Portugália, sem Spanyolország, sem Görögország, sem Törökország nem mondhat el magáról. Ráadásul a gazdasági problémák ellenére az olasz hadsereget is sikerült megerősíteni, Bár a szárazföldi haderő fejlesztése végül nem kapott akkora hangsúlyt, amekkorát szerettek volna neki szánni, de az amerikai és német segítségnek köszönhetően mind a haditengerészetet, mind a légierőt sikerült modernizálni. Ezek figyelembe vételével kijelenthető, hogy még akkor is, ha Olaszország nem számított a Szövetség legerősebb tagjának, a NATO „leggyengébb láncszeme" kifejezés nem állja meg a helyét vele kapcsolatban.

Felhasznált irodalom:

- ANDERLE Ádám: Spanyolország története. Panonica Kiadó, Budapest, 1999.
- BALOGH Ádám: Fejezetek Görögország újkori történetéből (A szabadságharctól napjainkig); Magyarországi Görögök Kulturális Egyesülete Csongrád Megyei Helyi Csoport, Szeged, 2013.
- BALOGH András: Bevezetés Délkelet-Ázsia történelmébe; ELTE Eötvös Kiadó, Budapest, 2015.
- BUTTIGNON, Ivan – ZENONI, Mattia: M.S.I. e terrorismo nero tra verità e montature. I collateralismi tra il partito neofascista e le organizzazioni armate di estrema destra; Solfanelli, 2014.
- CHIARINI, Roberto: A Movimento Sociale Italiano – történeti áttekintés; In: FEITL István (Szerk.): Jobboldali radikalizmusok tegnap és ma; Napvilág Kiadó, Budapest, 1998.

[106] HORVÁTH – PARAGI – CSICSMANN i. m. pp. 212-214.

- DE LUTIIS, Giuseppe: I servizi segreti in Italia. Dal fascismo alla seconda repubblica; Editori Riuniti, Róma, 1998.
- DR. DEMETER György (Szerk.): NATO kézikönyv; Stratégiai és Védelmi Kutatóintézet és NATO Információs és Sajtóiroda, Budapest, 1999.
- FISCHER Ferenc: A megosztott világ. A Kelet-Nyugat, Észak-Dél nemzetközi kapcsolatok fő vonásai 1941-1991.; Budapest, 1996.
- FLESCH István: A Török Köztársaság története; Corvina Kiadó, Budapest, 2007.
- FÖLDESI Margit – STELLA Szonja: Egy másik vesztes; Olaszország 1943-1947. Kairosz Kiadó, Budapest, 2006.
- GAMBIN, Kenneth (Szerk.): Malta. Roots of a nation. The development of Malta from an island people to an island nation; Midsea Books Ltd, 2004.
- GAZDAG Ferenc: Franciaország története 1945-1995. Zrínyi Kiadó, 1996.
- GÖMÖRI Endre: Makariosz; Kossuth Könyvkiadó, Budapest, 1973.
- HORVÁTH Jenő – PARAGI Beáta – CSICSMANN László: Nemzetközi kapcsolatok története 1941-1991; Antall József Tudásközpont, Budapest, 2014.
- HORVÁTH Jenő: Követő külpolitika. Az olasz EUrópa-politika a második világháború után; In: KISS J. László (Szerk.): A tizenötök Európái. Közösségi politikák – nemzeti politikák; Osiris Kiadó, Budapest, 2000.
- ILS AGA NATO series [Report on Warsaw Pact] Presentation about the information (Intelligence) concerning Warsaw Pact's military potential, explained at the meeting of NATO Defence Planning Committee, Brüsszel, 1972. május 24. https://digitalarchive.wilsoncenter.org/document/145156 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series General Staff of Defense (SMD) summary report about the meeting of NATO Defense Planning Committee at the ministerial session (Bruxelles, may 24th 1972), Brüsszel, 1972. július 6. https://digitalarchive.wilsoncenter.org/document/145155 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series General Staff of Defense (SMD) summary report of the ministerial meeting of the NATO Defense Planning Committee (Bruxelles, december 6th 1972), sent by Minister of Defense Tanassi to Prime Minister Andreotti, Brüsszel, 1973. január 24. https://digitalarchive.wilsoncenter.org/document/145159 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Memorandum by Cheef of Defense Staff, „Political-military considerations with regards to the ministerial meeting of the NATO Defense Planning Committee" (DPC), Brüsszel, 1972. május 24. https://digitalarchive.wilsoncenter.org/document/145154 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Memorandum by Chief of Defense Staff Aldo Ross to Minister of Defense, „32nd Meeting of the Military Committee – SHAPEX 64 – conversation with General Taylor"; Brüsszel, 1964. június 16. https://digitalarchive.wilsoncenter.org/document/155302 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Memorandum by Ministry of Defense, „NATO strategy", Brüsszel, 1963. december 10. https://digitalarchive.wilsoncenter.org/document/155300 (Letöltés ideje: 2022. 04. 19.)

- ILS AGA NATO series Memorandum by Ministry of Foreign Affairs, „Multilateral Nuclear Force", Brüsszel, 1964. https://digitalarchive.wilsoncenter.org/document/155307 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Message by Ministry of Foreign Affairs, Directorate General for Political Affairs and Security (DGAP), „NATO strategy", Brüsszel, 1963. december 4. https://digitalarchive.wilsoncenter.org/document/155301 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Note assessing Italian Strategic Vulnerability, Brüsszel, 1961. március 8. https://digitalarchive.wilsoncenter.org/document/155277 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Report by Ambassador Quaroni to Minister of Foreign Affairs Piccioni, „General de Martino's candidacy and Standing Group", Brüsszel, 1963. július 9. https://digitalarchive.wilsoncenter.org/document/155297 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Report by Permanent Representation to NATO Alessandrini to Minister of Defense Andreotti, Brüsszel, 1963. január 3. https://digitalarchive.wilsoncenter.org/document/155295 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Report, „Legitimacy, situation and prospects of the Atlantic Alliance", Brüsszel, 1969. https://digitalarchive.wilsoncenter.org/document/165234 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Report, „NATO conference on Intelligence (AHIWG) for the review of the documents MC 161/73 and 255/73 (Bruxelles, 25th March – 5th april)", Brüsszel, 1974. április 30. https://digitalarchive.wilsoncenter.org/document/155227 (Letöltés ideje: 2022. 04. 19.)
- ILS AGA NATO series Report, „Point 2. NATO situation", Brüsszel, 1963. https://digitalarchive.wilsoncenter.org/document/155294 (Letöltés ideje: 2022. 04. 19.)
- Istituto Luigi Sturzo Archivio Giulio Andreotti (ILS AGA) NATO series Memorandum by General Staff of Defense (SMD) to the Minister, NATO reorganization, 1965. december 29. https://digitalarchive.wilsoncenter.org/document/165226 (Letöltés ideje: 2022. 04. 19.)
- KERESZTY András: Tények könyve: NATO; Greger-Delacroix, Budapest, 1997.
- MAGYARICS Tamás: Az Amerikai Egyesült Államok története, 1914-1991. Kossuth Kiadó, Budapest, 2008.
- MAMMARELLA, Giuseppe – CACACE, Paolo: La politica estera dell'Italia. Dallo stato unitario ai gorni nostri. Editori Laterza, Róma, 2010.
- MAMMARELLA, Giuseppe: L'Italia contemporanea (1943- 2011); Società editrice il Mulino, Bologna, 2012.
- MINOLFI, Salvatore: Italia, Europa e Stati Uniti: La NATO dal 1969 al 1989; In: MINOLFI, Salvatore (Szerk.): L'Italia e la NATO. Una politica estera nelle maglie dell'alleanza; CUEN, Nápoly, 1993.
- National Archives (NA) Ministry of Defence, Chiefs of Staff Committee, 1973. január 23. https://www.nationalarchives.gov.uk/ (Letöltés ideje: 2022. 06. 14.)
- PACINI, Giacomo: Il cuore occulto del potere. Storia dell'Ufficio Affari riservati del Viminale (1919-1984); Nutrimenti, Róma, 2011.

- PÁL István: A londoni kiküldetés; A Katonai Felderítő Szolgálat Nagy-Britanniában szerzett operatív tapasztalatai a 70-es évek második felében; In: PÁL István – SZÉKELY Gábor (Szerk.): Az Eiffel- torony árnyékában. Majoros István 70 éves; ELTE BTK Új- és Jelenkori Egyetemes Történeti Tanszék, Budapest, 2019.
- SHENNAN, Andrew: De Gaulle; Akadémiai Kiadó, Budapest, 1997.
- SILVESTRI, Stefano: Il dibattito sulla non-proliferazione nucleare; In: MERLINI, Cesare (Szerk.): La politica estera dell'Italia. Cinquant'anni dell'Istituto Affari Internazionali; Società editrice il Mulino, Bologna, 2016.
- STEPHEN, Michael: The Cyprus question. A concise to the history, politics, and law of the Cyprus Question; Meto Print, London, 2001.
- SZABÓ Tibor: Olaszország politikatörténete 1861-2011. Belvedere Meridionale, Szeged, 2012.
- SZILÁGYI István: Portugália a huszadik században; L'Harmattan Kiadó, Budapest, 2015.
- TRANFAGLIA, Nicola: Anatomia dell'Italia repubblicana 1943-2009. Passigli Editori, Firenze, 2010.
- VALKI László (szerk): A NATO. Történet, szervezet, stratégia, bővítés; Corvina Kiadó, Budapest, 1999.

Levéltári dokumentumok:

- ÁBTL 3.2.3 Mt-867/1. p. 118. – Információs jelentés, Róma, 1967. augusztus 15.
- ÁBTL 3.2.3 Mt-867/2. p. 109. – Információs jelentés, Róma, 1968. november 26.
- ÁBTL 3.2.3 Mt-867/2. p. 87. – Információs jelentés, 1968. szeptember 3.
- ÁBTL 3.2.3 Mt-867/3. p. 22. – Információs jelentés, Róma, 1969. november 5.
- ÁBTL 3.2.3. Mt 867/1. p. 112. – Információs jelentés, Róma, 1967. augusztus 15.
- ÁBTL 3.2.3. Mt 867/8. p. 16. – Információs jelentés, Róma, 1971. március 18.
- ÁBTL 3.2.3. Mt-867/10. p. 206. – Feljegyzés, Budapest, 1972. július 5.
- ÁBTL 3.2.3. Mt-867/11. p. 34. – Információs jelentés, Budapest, 1972. december 15.
- ÁBTL 3.2.3. Mt-867/11. p. 61. – Információs jelentés, Róma, 1973. április 9.
- ÁBTL 3.2.3. Mt-867/2. p. 104. – Információs jelentés, Róma, 1968. november 13.
- ÁBTL 3.2.3. Mt-867/2. p. 70. – Jelentés, Róma, 1968. július 10.
- ÁBTL 3.2.3. Mt-867/2. p. 80. – Jelentés, Róma, 1968. július 10.
- ÁBTL 3.2.3. Mt-867/6. p. 116. – Információs jelentés, Róma, 1970. szeptember 10.
- ÁBTL 3.2.3. Mt-867/7. p. 14. – Információs jelentés, Róma, 1970. október 23.
- ÁBTL 3.2.3. Mt-867/7. p. 71. – Információs jelentés, Róma, 1970. december 11.
- ÁBTL 3.2.3. Mt-867/8. p. 131/128-130. AIPE-jelentés
- ÁBTL Mt-867/1. p. 118. – Információs jelentés, Róma, 1967. december 27.
- ÁBTL 3.2.3 Mt-867/2. p. 34-37. – Információs jelentés, Róma, 1968. június 15.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1970/69. doboz – Jelentés, Róma, 1970. december 2. p. 1.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1975/110. doboz – Jelentés, Róma, 1975. március 8. pp. 1-5.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1972/82. doboz – Jelentés, Róma, 1972. január 20. p. 3.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1972/82. doboz – Jelentés, Róma, 1972. január 20. p. 5.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1972/82. doboz – Jelentés, Róma, 1972. június 29. p. 1.

- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Jelentés, Róma, 1974. október 11. p. 2.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Jelentés, Róma, 1974. szeptember 30. p. 1.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Jelentés, Róma, 1974. október 11. p. 1-2.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 8.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 16.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 19.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 17.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében. A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 18.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében. A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 18-24.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében; A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. p. 25.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. doboz – Olaszország katonapolitikai helyzete a belpolitikai és a nemzetközi tényezők tükrében. A Magyar Néphadsereg Vezérkara 2. Csoportfőnökségjelentése, 1974. október 29. pp. 26-28.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. p. 19.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1974/91. p. 19.
- MNL OL XIX-J-1-j Olaszország KÜM TÜK 1975/108. doboz – Jelentés, Róma, 1975. január 27. p. 5.

BIHARI RITA

A KONFLIKTUSFORMÁCIÓTÓL A BIZTONSÁGI KÖZÖSSÉGIG – A NYUGAT-BALKÁNI REGIONÁLIS BIZTONSÁGI EGYÜTTMŰKÖDÉS FEJLŐDÉSE

Bevezetés

Elméleti áttekintés

A biztonsági közösséget leginkább úgy írhatjuk le, mint egy integrálódott csoportot, ahol az integráció egyet jelent a közösség érzésének, azaz a közös „mi" tudatnak az elérésével, amelyet formális és informális intézmények vagy gyakorlatok kísérnek akképpen, hogy mindeközben hosszú távon megteremti a békés változást a csoport tagjai között.[1] Ahogy a biztonsági közösséggel foglalkozó irodalom gyarapodott, úgy változott a fogalom meghatározása is. Idővel a kutatók a fogalom eredeti alkalmazási körétől eltértek, hogy azt jobban adaptálhatóvá tegyék a nemzetközi kapcsolatok tanulmányozására. A biztonsági közösség konstruált egységként fogható fel,[2] egészen egyszerűen egy olyan régió, amelyben erőszak és háború egyáltalán nem vagy nagyon ritkán válik alkalmazottá.

De vajon mire van szükség a békés államközi kapcsolatok biztosításához? Ahogy a biztonság természete és definíciója az idők során változott, úgy változott a béke jelentése, a fenyegetés, valamint az államok, társadalmak és más szereplők közötti békéhez szükséges feltételek fogalmi meghatározása.[3] A biztonsági közösség elméleti koncepcióját Karl Deutsch írta meg 1957-ben.[4] Úttörő munkája a *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience, (Politikai közösségek és az észak-atlanti térség: Nemzetközi szervezet a történelmi tapasztalatok tükrében)*[5] címet viseli. Olyan alapmű, ahol Deutsch azt állítja, hogy a biztonsági közösség felfogható olyan embercsoportként, amely a közös társadalmi problémákat, képes és törekszik megoldani a békés változás eszközeivel és folyamataival. A szerző összevont és pluralista közösségekről beszél

[1] DEUTSCH, Karl Wolfgang: Political Community and the North American Area: International Organization in the Light of Historical Experience; Princeton University Press, Princeton, 1957. p.33.

[2] „*A biztonsági közösség fogalma osztja a nemzetközi kapcsolatok konstruktivista eléletének két alapvető premisszáját, miszerint az államok rendszerének kulcsstruktúrái inkább interszubjektívek, mint materiálisak, hogy az állami identitásokat és érdekeket jelentős részben ezek a társadalmi struktúrák konstruálják, nem pedig az emberi természet vagy a belpolitika által a rendszer számára exogén módon adottak."* Lásd: ACHARYA, Amitav: Collective identity and Conflict management in Southeast Asia; In: ADLER, Emanuel–BARNETT, Michael (eds.): Security Communities; Cambridge University Press, Cambridge, 1998.

[3] JAKESEVIC, Ruzica: Security Community Building In The Western Balkans – Wishful Thinking Or An Inevitable Future? Teorija In Praksa let. 56, 2019/1. https://www.fdv.uni-lj.si/docs/default-source/tip/vzpostavljanje-varnostne-skupnosti-na-zahodnem-balkanu-lepa-%C5%BEelja-ali-neogibna-prihodnost.pdf?sfvrsn=0 (Letöltés ideje: 2022. 05. 02.)

[4] A biztonsági közösség kifejezést elsőként Richard van Wagenen használta 1952-ben.

[5] DEUTSCH i. m.

művében. Esetünkben az utóbbi lehet számottevő hiszen az integráció vezet el egy pluralista biztonsági közösség létrejöttéhez, melyeket Deutsch érvelése szerint könnyebb létrehozni és fenntartani, mint összevont társaikat. Deutsch két feltételt azonosított. Először is, hogy az érintett kormányok erőszak nélkül tudjanak gyorsan reagálni egymás szükségleteire. Másodszor pedig az, hogy legyenek a közösség tagjainak politikailag is összeegyeztethető értékei. Deutsch tehát röviden azt állította, hogy azok az államok, amelyek egy biztonsági közösségben élnek, nem egyszerűen stabil rendet teremtenek, hanem stabil békét is.

A hidegháború vége után Emanuel Adler, Michael Barnett, Raimo Väyrynen, Andrej Tusicisny, Michael Haas és Carol Weaver is tovább dolgozták az elméletet. Kétségtelenül legnagyobb hatású Adler-Barnett 1998-ra datálható könyve a *Security Communities,*[6] avagy *Biztonsági Közösségek* volt, amely lendületet adott a kutatási területnek. Újradefiniálták a biztonsági közösséget, mint sokoldalú közvetlen kölcsönhatásokon és kölcsönös hosszú távú érdekeken alapuló kapcsolatot. Adler és Barnett megfogalmazta a biztonsági közösség evolúciós folyamatát is. Azt állítják, hogy egy születő biztonsági közösség megfelel a békés változás alapvető elvárásainak, amíg a kiforrott közösség jellemzői között megtalálható a kollektív biztonsági mechanizmus, a nemzetekfelettiség, a transznacionalitás. A biztonsági közösségek viszonyát pedig az integrációtól teszik függővé, hogy az lazán vagy szorosan összekapcsolt. A bemutatott keretrendszer Deutsch eredeti koncepciójának legjavát használja ki, és hiányosságait korrigálja azáltal, hogy a szociológiai és nemzetközi kapcsolatok elméletének négy évtizedes lényeges meglátásait és különféle empirikus tanulmányokat kölcsönöz, amelyek a biztonsági közösségek koncepciójából származtak.

Raimo Väyrynen[7] szintén érdemel egy rövid említést, mivel megfogalmazta azt a különbséget, amely az államközi biztonsági közösségek és az átfogó biztonsági közösségek között húzódik. Ennek alapján a nyugat-európai közösséget az átfogó kategóriába sorolta, amely az államközi konfliktusokat és a polgárháborúkat is elképzelhetetlennek tartják.

Carol Weaver,[8] akit ugyancsak egy mondat erejéig említenék, kifejtette, hogy a biztonsági közösségeknek kiegyensúlyozott multipolaritáson kell alapulniuk ahhoz, hogy létrejöhessenek és fennmaradhassanak. A biztonsági közösség vizsgálata több problémába ütközik, mivel fontos, ám olykor megfoghatatlan fogalmakkal operál, mint a közösség, a békés változás elvárásai, a kormányzás, az institucionalisták által fontosnak vélt intézményi szerep. Adler és Barnett nyomán így a definíciós térképet és a biztonsági közösségek kialakulásának szintjeit kell meghatározni. Nevezetesen az ösztönzőket, a strukturális elemeket, valamint ezen szintek közötti változók kölcsönhatását, amelyek elvezetnek a bizalom és a kollektív identitás kialakulásához.

---

6 ADLER, Emanuel – BARNETT, Michael: Security Communities; Cambridge University Press, Cambridge, 1998.

7 VÄYRYNEN, Raimo: Stable Peace Through Security Communities? Step towards Theory-Building; University of Notre Dame, the Joan B. Kroc Institute For International Peace Studies. 2000.

8 WEAVER, Carol: Black Sea Regional Security: present multipolarity and future possibilities; European Security, 2011/1. pp. 1-19.

Természetesen a klasszikus elméleti alapvetések és fejlesztések képviselőin túl több kutató is foglalkozott, illetve foglalkozik a biztonsági közösség jelenségével, így többek között pld. Sonja Stojanovic Gajic és Filip Ejdus,[9] Ruzica Jakesevic,[10] Suzette Grillot, Valerie J. D'Erman, Rebecca J. Cruise,[11] Jovana Milovanovic.[12]

A teljesség igénye nélkül a tanulmány során mindezen elméleti alapvetések figyelembevételével vizsgálom a nyugat-balkáni biztonsági közösség lehetőségét, és relevancia esetén evolúcióját.

Hogyan születnek a biztonsági közösségek?

A biztonsági közösség fogalma a közelmúltban túllépett a tudományos diskurzuson, és a politikaformálás területére is eljutott. A hidegháborút követően már a NATO is úgy határozta meg magát, mint transzatlanti biztonsági közösség. 2003-ban az ASEAN szándéknyilatkozatot adott ki, amelyben biztonsági közösségként utalt önmagára, és az EBESZ[13] is megfogalmazta biztonsági közösség építési céljait.[14] Alapvetően viszont azt mondhatjuk, hogy inkább a tudományos megalapozottság és a nemzetközi kapcsolatok területére korlátozódik a jelenség. Miközben a nemzetközi kapcsolatokban is perifériára szorul, amit azzal magyarázhatunk, hogy a közösség logikája megkérdőjelezi az anarchia[15] logikáját. Ha az államok szórványosan törekednek a biztonsági együttműködésre, a nemzetközi rend anarchikus jellege miatt úgyis hangsúlyeltolódás tapasztalható az önsegélyező, önérdekkövető, előnyteremtő magatartásra a társakkal szemben.[16]

A „hogyan születnek?" kérdést körbejárva, az bizonyos, hogy Adler és Barnett, Sheenan és Acharya is megfogalmazta azon feltételeket, amelyek mentén a közösségek, illetve a biztonsági közösségek kialakulhatnak. Adler-Barnett három

---

9 STOJANVIC-GAJIC, Sonja – EJDUS, Philipp (eds.): Security Community Practices in the Western Balkans; Routledge, 2018

10 JAKESEVIC i. m.

11 GRILLOT, Suzette – D'ERMAN, Valerie J. – CRUISE, Rebecca J.: Developing Security Community in the Western Balkans: The Role of the EU and NATO Paper prepared for the EUSA; Tenth Biennial International Conference May 17-19, 2007. Montréal, QC, Canada Panel 1J: CSFP Case Studies; http://aei.pitt.edu/7789/1/cruise-r-01j.pdf (Letöltés ideje: 2022. 05. 02.)

12 MILANOVIĆ, Jovana: Liberalizam I Bezbednosne Zajednice: Evropska Bezbednosna Zajednica Na Zapadnom Balkanu; Politicka revija, 2016/3. pp.41-58.

13 Részleteket lásd REMEK, Éva: Az EBESZ – a biztonsági közösségépítés modellje; Budapest, Dialóg Campus Kiadó, 2018.

14 KOSCHUT, Simon: Regional order and peaceful change: Security communities as a via media in International Relations Theory. Cooperation and Conflict; Zeppelin University, Germany, 2014/4.

15 Az anarchia meghatározása jelen esetben nem a szó hétköznapi, hanem nemzetközi kapcsolatok szempontjából releváns értelemben történik. Ennek megfelelően az államok rákényszerülnek a saját biztonságuk garantálására. Az államok egy felsőbb nemzetközi hatalom (pl: világkormány) hiányában kénytelenek konfliktusba kerülni egymással, ugyanis maguknak kell gondoskodniuk saját biztonságukról, semmiféle más entitás ezt nem teszi meg. Lásd: BALOGH, István: Biztonságelméletek; Nemzet és Biztonság, 2013/3-4. p. 41.

16 KOSCHUT i. m.

szintet különböztet meg, miszerint a kiváltó körülmények ösztönzik, és egymás irányába tolják az államokat, amelyek ezáltal politikáikat összehangolják. A társadalmi tanulás folyamata a második szint, amelyben a hatalom és az eszmék strukturális elemei dominálnak. A harmadik szint a kölcsönös bizalom és a kollektív identitás kialakulásának terepe, ami az első két változó pozitív kölcsönhatása révén jön el.[17] Sheenan[18] három feltételt azonosít, ez alapján szükség van összeegyeztethető politikai értékekre, másodszor politikai és egyéb kommunikációs hálózat létrejöttére, harmadszor pedig dinamikus kapcsolat kell legyen az első két feltétel között. Acharya szerint külső kényszerítő hatás révén is eljuthatunk a biztonsági közösség születéséig, amihez tulajdonképpen egy sor fenyegetésre van szükség, amelyet a leendő közösség tagjai egyaránt biztonságukat veszélyeztető tényezőként percepcionálnak.[19] Következtetésként levonható, hogy a biztonsági közösségek társadalmilag konstruáltak, és az idő távlatával fejlődnek a születés–növekedés–érettség vonalon, kiváltó mechanizmusa pedig lehet egyrészt normatív, tehát közös együttműködés elképzelése, vagy anyagi, azaz közös fenyegetés.[20]

A regionális biztonsági dinamika alakulása és az együttműködés fejlődése a Nyugat-Balkánon

Konfliktusformáció

Az 1991 utáni események már jelezték a regionális konfliktusformáció kialakulását a Balkán-félszigeten. A balkáni alkomplexumnak Albánián és Szlovénián kívül minden jugoszláv állam állandó tagja volt, amelyek a délszláv háború hatására betagozódtak a regionális konfliktusformációba. Jugoszlávia és Albánia biztonsági helyzetét tekintve kölcsönös egymásrautaltságot mutattak a hidegháború után is. Bár Albánia nem volt része a délszláv háborúk okozta erőszaknak, mégis a részkomplexum egyik pólusává vált, köszönhetően annak, hogy a posztjugoszláv térrel kapcsolatok egész sorát tartotta fenn.[21]

Ami a nyugat-balkáni konfliktusok természetét illeti, elmondható, hogy azok egyre erőszakosabb voltában szerepet játszott a nemzetközi közösség inaktív magatartása is. A hidegháború végén, és a keleti blokk felbomlását követően a nagyhatalmak óvatosan közelítettek minden olyan változáshoz, amely destabilizálhatja a nemzetközi rendszert.[22] A be nem avatkozás politikáját folytatva az állapítható meg, hogy a nemzetközi közösség nem volt felkészülve a következmények kezelésére.

---

17 ADLER – BARNETT i. m. p.29.

18 SHEENAN, Michael: International security; Lynne Rienner Publishers; Boulder, Colorado, 2005.

19 ACHARYA, Amitav: Constructing a Security Community in Southeast Asia: ASEAN and the Problem of Regional Order; Politics in Asia, Routledge, 2000. pp. 34-35.

20 ADLER – BARNETT i. m. pp. 49-52.

21 PUGH, Michael – COOPER, Neil – GOODHAND, Jonathan: War Economies in a Regional Context: Challenges of Transformation; Lynne Rienner, Boulder and London, 2004. p. 147.

22 GLAURDIC, Josip: The Hour of Europe; Yale University Press, New Haven, Connecticut, 2011. p .9.

Elsőként az Európai Közösség reagált a konfliktus kiigazítását megcélzó törekvésekkel kapcsolatban 1991-ben,[23] azonban 1993-ban a Maastrichti Szerződéssel az Európai Közösség átalakult Európai Unióvá, és egyelőre hiányoztak a megfelelő eszközök, a hatékony kül- és biztonságpolitika és a régió stabilizálásához elengedhetetlen katonai erő. Ennek hatására az USA továbbra is központi szerepet töltött be az események koordinálásában, amely eredményeként megszületett a Daytoni Békeszerződés, és az erőszakos cselekmények mellett véget vetett az 1991 óta követett visszaszorítási stratégiának is a Balkánon. Bizonyos, hogy 1991 és 1995 között a balkáni részkomplexum biztonsági helyzete belülről irányított volt,[24] viszont 1995 után a helyi szereplők a külföldi kormányoktól és a nemzetközi szervezetektől érkező támogatásban bíztak, ezáltal a jugoszláv utódállamok kevésbé keresték a kompromisszumokat egymással, és nem is engedték a külső szereplők feltétlen elszakadását a nyugat-balkáni eseményektől.[25]

A regionális konfliktusformációra egyfajta összetett természet jellemző, amelyet hálózatok egész sora bonyolít tovább.[26] Ezek a hálózatok a Nyugat-Balkán esetében is megmutatták magukat gazdasági, katonai, politikai és társadalmi definiáltságukban, amelyek nem csak a régiót kötötték össze, hanem az európai regionális biztonsági komplexummal is összekapcsolták a konfliktusképződményt.[27] A politikai hálózatok az 1990-es években alakultak ki és fokozatosan bővültek újabb politikai hálózatok kialakulásával. A balkáni alkomplexum gazdasági és katonai hálózatai 1991 és 1995 között szorosan kapcsolódtak a politikai hálózatokkal, és olyan magas szinten kötődtek egymáshoz, hogy értelmezni azokat tulajdonképpen csak együtt lehetséges. Természetesen a rossz gazdasági feltételek és az erőszak kialakulása közötti kapcsolat sokáig nem volt felismerhető, vagy az elemzések során is figyelmen kívül hagyták, miközben ma már biztosan állítható, hogy a balkáni erőszakot megelőzte egy évtizedes gazdasági válság.[28] Mindez pedig a balkáni részkomplexum fejlődésére is kihatással volt. Értve ezalatt az árnyékgazdaságokat, a titkos gazdasági tevékenységeket, határon átnyúló szervezett bűnözői hálózatokat, illetve a fegyver- és embercsempészetet, amelyek a mai napig a Nyugat-Balkán megoldatlan problémáit képezik.[29] A politikai, gazdasági, katonai és társadalmi hálózatok elszaporodása a részkomplexumban kettős hatással bírtak. Habár a régiót összefogta, és azt összekapcsolta az európai regionális biztonsági komplexummal, az egyesített regionális konfliktusforma tagjai túlnyomórészt negatív biztonsági dinamikát mutattak.

---

[23] RIDING, Alan: Conflict in Yugoslavia: Europeans Send High-Level Team; New York Times, 1991. http://www.nytimes.com/1991/06/29/world/conflict-in-yugoslavia-europeanssend-high-level-team.html (Letöltés ideje: 2022. 05. 02.)

[24] BUZAN, Barry – WAEVER, Ole: Regions and Powers: The Structure of International Security; Cambridge University Press, Cambridge, 2003. p. 383.

[25] Uo.

[26] ARMSTRONG, Andrea – RUBIN, Barnett.: Policy Approaches to Regional Conflict Formations; Centre on International Cooperation, New York, 2002. pp. 1-16.

[27] PUGH – COOPER – GOODHAND i.m.

[28] STRAZZARI, Francesco – COTICCHIA, Fabrizio: The Phantom Menace. Transnational Organized Crime and the Shaping of the Western Balkans; In: SOLIOZ, C.– STUBBS, P. (eds.): Towards Open Regionalism in South East Europe; Nomos Publishers, Baden-Baden, 2012. p. 149.

[29] BECHEV, Dimitar: Constructing South East Europe. Houndmills, Basingstoke, Hampshire; Palgrave Macmillan, 2011. p. 37.

A háború megszűnése után a térség lassan stabilizálódni kezdett. A legtöbb nyugat-balkáni állam visszaállította az erőszakmonopólium intézményét, és megszakította kapcsolatait a félkatonai és irreguláris erőkkel, ezzel pedig az említett politikai és katonai hálózatok egy részét megszüntette.[30] Gazdasági vonalon az illegális gazdasági hálózatok viszont továbbra is aktívak maradtak. Az erőszak megállítása és a viszonylagos lassú fejlődés arra engedte következtetni a nemzetközi közösséget, hogy a balkáni regionális konfliktusok feloldódhatnak, és közelebb kerülhetnek a biztonsági egymásrautaltság baráti pólusához. 1995-től a regionalitás figyelembevételével megnyíltak a külső beavatkozás csatornái is a régióban, viszont még kérdéses volt, hogy mi alkotja a régiót, így számos kívülről vezérelt regionális kezdeményezés indult meg a délkelet-európai államok felé. Ami pedig ennél is meglepőbb, hogy a nyugat-balkáni regionális biztonságot továbbra is elkülönültnek tekintették Európa többi részétől. Az ezredfordulóval az EU viszont a régió vezető biztonsági szereplője kezdett lenni, így koherenciát vállalva a Nyugat-Balkánnal. A régió és tágabb környezetének biztonsága ezáltal kapcsolódott össze. Ezt megelőzően voltak próbálkozások, pressziók annak vonatkozásában, hogy a régió tagjait rábírják a kölcsönös biztonsági kapcsolatok kiépítésére. A Balkán 1991-1995 között konfliktus-képződményként volt definiálható, túlnyomórészt negatív jellegű regionális egymásrautaltsággal, amelyek döntően hazai tényezőkre vezethetőek vissza, addig a térség államai külső hatalmak hatására kezdtek távolodni a konfliktustól és haladtak a biztonsági rezsim kialakítása felé.

Biztonsági rezsim

A biztonsági rezsimet amennyiben érteni kívánjuk, azt Robert Jervis által tehetjük meg, ugyanis legrészletesebben ő foglalkozott vele 1982-ben írt munkájában.[31] A biztonsági rezsimek, avagy a biztonsági rendszerek számára öt olyan tulajdonságot azonosított, amely a biztonsági rendszert kiemeli a környezetéből. Ez az öt: a biztonság elsőbbsége, a versengő jellege, a bizonytalanság, az állam biztonsági szükséglete, és ennek viszonyában, hogy mekkora biztonsággal rendelkezik az adott állam.[32] Ahhoz, hogy sok más célt megvalósítsunk, először garantálni kell a biztonságot, viszont többnyire az érintett felek nagyon óvatosan közelítenek a biztonsági rezsimbe történő belépés kapcsán. A bizalom ugyanis nem rögzül olyan mélyen egy biztonsági rezsim vonatkozásában, mint egy biztonsági közösség esetében. Ez következtethető abból, hogy saját biztonsági szektoruk bővítése továbbra is fennáll, és elsősorban a saját maguk védelmében reagálnak. A biztonsági szférában tapasztalható versengés hozzájárul a funkcionális biztonsági rezsimek felállításának nehézségéhez. A biztonsági rezsimben a legkisebb hibáknak is beláthatatlan következményei lehetnek. Ha egy tag úgy dönt, hogy eltér a rezsimet meghatározó normáktól és szabályoktól, akkor a rezsim többi tagjának biztonsága is kérdésessé válik. A biztonságot így a biztonsági rezsimben nagyobb bizonytalanság jellemzi, mint a nemzetközi kapcsolatok egyéb területein. A biztonsági rezsimek tehát egyszerre értékesek és nehezen megvalósíthatóak, mindazonáltal, amennyiben nem adott kérdéshez kapcsolódó, hanem általános biztonsági együttműködésről beszélünk, igen ritkák is, pedig elérése esetén békét és stabilitást hozhatnak.

---

30 KALDOR, Mary: New and Old Wars; Polity Press, Cambridge, 2012. p. 57.
31 JERVIS, Robert: Security regimes; International Organization, 1982/2. pp. 357-378.
32 Uo. p. 359.

Ebből következtetve megállapíthatjuk, hogy a biztonsági közösség felé vezető úton a biztonsági rezsimek jelenthetik a kezdeti lépést. Mivel magatartásukat normák, elvek, szabályok korlátozzák, biztonságos és békés környezetet biztosítanak. Ez a környezet pedig kedvez annak a fejlesztésnek, amelynek eredménye lehet egy összetartó közösség. Mindenképp nyomatékosítani kell azt a tényt, hogy a biztonsági rezsimek, rendszerek és a biztonsági közösség fogalmak nem összetévesztendőek. A biztonsági közösség szereplői alapvetően egy egyértelmű és hosszú távú érdekkonvergencia részesei, amíg a biztonsági rezsimben a biztonsági dilemma, a versengő fegyverkezés, a vészhelyzeti tervezés általában folytatódik, habár a fegyverek és katonai képességek terjedését igyekeznek korlátok közé szorítani. A szereplők érdekei tehát nem összehangoltak, és nem is teljes mértékben versengőek.[33] Tulajdonképpen egy ellenséges viszonyban is kialakulhat, ahol az erőegyensúly vagy a kölcsönös elrettentés gátolja az erő alkalmazását, és nincs benne a kollektív identitás és a csoporthoztartozás érzése, mint a biztonsági közösségekben.[34]

A posztjugoszláv tér esetében a regionális megközelítés első kísérlete 1992-ben az ENSZ-hez köthető. A regionális megközelítés viszont csak 1995-1996-ban vált olyan normává, amelyet a külső szereplők alkalmaztak a balkáni konfliktusok megoldási törekvéseiben. Több megállapodás és kezdeményezés vált alapvető eszközzé, amelyek a térség stabilizálásának kulcselemét biztosították. A legfontosabb a Daytoni Békeszerződés, amelyben az úgynevezett „kemény biztonság" kapott prioritást, azonban a fegyverzetellenőrzésre és a bizalomerősítő intézkedésekre vonatkozó javaslatokat is tartalmazott annak érdekében, hogy csökkentse a jövőbeni konfliktusok kialakulásának kockázatát. Ez a megállapodás tekinthető szinte az első olyan stratégiailag fontos dokumentumnak, amely a korábbi ellenfelek közötti biztonsági kapcsolatok javítására és a viszonosság előmozdítására törekedett.[35]

1996-ban a Jugoszláv Szövetségi Köztársaság, Horvátország és Bosznia-Hercegovina aláírta azt a Firenzei Megállapodást, amely a szubregionális fegyverzetellenőrzésért felelt. A régióban fellelhető fegyverek számának csökkentésére vállalt kötelezettség javította az együttműködést, az átláthatóságot és a biztonsági kapcsolatok kiszámíthatóságát Délkelet-Európában.[36]

1996-ban a Daytoni Megállapodás és az EBESZ tevékenységének kiegészítéseként elindult a Regionális Megközelítés[37] (Regional Approach to the countries of South-Eastern Europe). Ez elsősorban a politikai és a gazdasági fellendülést igyekezett szolgálni a régióban olyan uniós eszközök támogatásával, mint a PHARE,[38] az OBNOVA,[39] illetve egyéb együttműködési és társulási megállapodások.

---

33 ACHARYA (1998) i. m. p.201.

34 ACHARYA (2000) i. m. p.19.

35 MCCAUSLAND, Jeffrey: Arms control and the Dayton Accords; European Security, 1997/2. p. 19.

36 OSCE: OSCE Marks 20th Anniversary of Sub-Regional Arms Control Agreement, 2016. http://www.osce.org/cio/246991 (Letöltés ideje: 2022. 05. 03.)

37 Az Európai Unió feltételesség elvén alapuló politikája a koherens és átláthatóbb nyugat-balkáni együttműködés érdekében.

38 A kelet-közép-európai országok közösségi támogatási programja.

39 A nyugat-balkáni államoknak nyújtott uniós segítség fő csatornája volt egészen 2001-ig, miután integrálták a CARDS-programba.

A SECI (South-East European Cooperative Initiative – Délkelet-európai Együttműködési Szervezet) szintén egy újabb stratégia volt, amely a régió stabilizálására hivatott, egy szélesebb földrajzi kiterjedésű hatókörrel, viszont hatálya fordított arányosságban meglehetősen korlátozott volt. A transznacionális biztonsági kihívások kezelése és az infrastruktúra fejlesztése által próbálta a regionális együttműködést segíteni.[40]

Kiemelendő, hogy habár helyi irányítású kezdeményezés a SEECP (South-East European Cooperation Process/Délkelet-európai Együttműködési Folyamat), mégis az előzőekben bemutatott Daytoni Békeszerződés, a Firenzei Megállapodás, a Regionális Megközelítés és a SECI voltak azok, amelyek a feltételesség és a közvetlen rákényszerítés eszközeivel támogatták a regionális együttműködés, a jószomszédi viszony, az átláthatóság és kölcsönösség elvét. Ezáltal a térséget biztonsági rezsimmé változtathatták volna, ugyanis normákat, szabályokat, elveket adott a régió országai számára, azokat azonban nem minden regionális szereplő fogadta el. A 1990-es évek eseményeire tekintettel a biztonsági rezsim kialakulásának meghiúsulása elsősorban azért csúszott meg, mert a háború öröksége még élénken élt ahhoz, hogy kölcsönösségről és bizalomról beszélhessünk a régiót alkotó tagok között. Másodsorban a kívülről irányító, mondhatni biztonsági szereplők között nem volt teljes az egyetértés, és a koordináció, mint cselekvési mechanizmus is hiányos volt. A balkáni régió mibenléte és annak megközelítése amennyiben és amíg kérdéses, addig a bevezetett regionális kezdeményezések sem válhatnak igazán hatékonnyá. Végül pedig a harmadik ok, hogy bár az európai biztonsági komplexum része a nyugat-balkáni alrégió, mégis Európától eltérő területként kezelték azt. A béke talán ennek hatására is, de rövid életűnek bizonyult. Az 1995 és 1999 között kezdeményezések nem hoztak létre biztonsági rendszert, azonban a biztonsági átalakulás nem állt meg, és jelentős fázisa tagadhatatlanul a koszovói konfliktussal kezdődött.

Biztonsági közösség

A koszovói konfliktus fordulópontot jelentett a térség biztonsági fejlődésében. Bármennyire is furcsa, de lehetőséget kínált a régió államai számára az európai biztonsági közösséghez történő közeledésre, csatlakozásra. Koszovó minden negatív hozadéka mellett felfedte a balkáni válságokra adott reaktív és szelektív válaszlépések korlátait.[41] A régiónak szüksége volt, hogy hosszú távú stratégiát kínáljanak annak fejlesztésére. A koszovói erőszak pedig rávilágított arra, hogy az addigi megközelítés sürgős újragondolására van szükség,[42] továbbá előtérbe helyezte, hogy a nyugat-balkáni államok egymásra vannak utalva, és hogy a Dayton után közvetlenül kialakult béke mennyire törékeny.[43] Így az újbóli konfliktus adott egy erőteljes lökést a balkániaknak, hogy az EU felelősségi körébe tartozzanak. Az EU aktívabb szereplő

[40] WATANABE, Lisa: Securing Europe; Palgrave Macmillan, Houndmills, Basingstoke, Hampshire, 2010. pp.131-132.

[41] VUCETIC, Srdjan: The Stability Pact for South Eastern Europe as a Security Community-Building Institution; Southeast European Politics, 2001/2. p. 116.

[42] BECHEV, Dimitar: Carrots, Sticks and Norms: the EU and Regional Cooperation in Southeast Europe; Journal of Southern Europe and the Balkans, 2006/1. p. 34.

[43] BECHEV (2011) i. m. p. 49.

lett a régióban, az integráció modelljét pedig újra a megbékélés és az emberi jogok érvényesülésének eszközévé tette.[44]

A legfontosabb és egyben első lépés a Délkelet-európai Stabilitási Paktum jelentette, a konfliktusmegelőzés hosszú távú proaktív megközelítését képviselte,[45] amely az integrációs politika és a délkelet-európai együttműködés kombinációján alapult.[46] Lényegében egy kísérlet volt egy olyan regionális biztonsági keret létrehozására, amely elősegíti a békés kapcsolatokat a jugoszláv utódállamok között, valamint tágabb környezetükkel is képesek ezt megvalósítani.[47]

A Stabilitási Paktum azonban több hiányossággal is rendelkezett, amelyek megakadályozták, hogy biztonsági közösségépítő potenciálja kiteljesedjen. A hiányosságok legjelentősebben a korlátozott erőforrások terén mutatkoztak meg,[48] illetve annak viszonylatában, hogy a Paktum az összes délkelet-európai államot megcélozta. Magának a Paktumnak a tulajdonosi köre is kétértelműséget hordozott azáltal, hogy egyszerre az EBESZ és az EU is érdekelt volt benne. Céljai nagyrészt elvontak és távoliak maradtak, mivel annak elérési, megvalósíthatósági mechanizmusai nem voltak tisztázottak. 1999-ben a Stabilitási Paktumra építve indították el a Stabilitási és Társulási Folyamatot (Stabilisation and Association Process – SAP), amely igyekezett kezelni a Stabilitási Paktum hiányosságait. Koordinátora kizárólag az EU volt, és céljaiban a nyugat-balkáni országokra orientálódott. Fő sodrásában az az elgondolás állt, hogy a nyugat-balkáni országok egymással és az Európai Unióval bilaterális, illetve multilaterális kapcsolatokat kívánnak teremteni.[49] Ennek eredményeként pedig az EU befolyási övezetébe vonja a balkáni részkomplexumot, és azt az európai biztonsági közösség részévé teszi. A regionalizáció ösztönzésére az EU természetesen egyéb más eszközt is alkalmazott. Ahogy nőtt a nyugat-balkáni államok uniós eszköztára, úgy csökkent a térségben a nagyszabású erőszak lehetősége. Az EU biztonsági helyzetre gyakorolt hatása tehát jelentős. Az EU arra tett kísérletet a régióban, hogy negatívról pozitívra változtassa a biztonsági kölcsönös függőség elterjedt mintáit. Továbbá rávilágított arra, ahogy a nyugat-balkáni államok politikai elitje szocializálódott az EU-val való összehangolt bel-és külpolitikai érdekében.

A szocializáció szintén egy eszköz a béke előmozdítására, a biztonsági közösségek kezdeti szakaszainak létrehozására. A normák, szabályok és értékek a belpolitikai döntéshozatal és a külpolitika alakításának mintáiként internalizálódnak.[50] Az EU a már említett kétoldalú, többoldalú és regionális

---

[44] SOLANA, Javier: SOLANA, Javier: Public Debate on Western Balkans. Intervention by High Representative of the Common Foreign and Security Policy to the General Affairs Council; Brussels, 2000. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/discours/gac%2010.7%20en.doc.html (Letöltés ideje: 2022. 05. 04.)

[45] WATANABE i. m. p. 135.

[46] BECHEV (2006) i. m. p.34.

[47] VUCETIC i. m. p.112.

[48] BECHEV (2011) i. m. p. 53.

[49] European Commission: The Stabilisation and Association process for Southeast Europe: First Annual Report; Brussels, COM(2002)163 final. pp. 9-11.

[50] KAVALSKI, Emilian: Extending the European Security Community; Tauris, London, 2008. p. 65.

kezdeményezések révén gyakorolta szocializációs hatalmát.[51] A nyugat-balkáni államok közötti pozitívabb irányú kapcsolatok a belpolitikai változások miatt alakultak ki, amelyeket az EU támogatott a kétoldalú szerződéses kapcsolatokon keresztül. Az EU politikája elsősorban a kapacitásfejlesztésre, az intézmények hatékonyságának növelésére és az eredményesség javítására irányultak. A külpolitikai gyakorlatban pedig törekedett a békés megközelítés bevezetésére és fenntartására.[52] Ez a folyamat indította el a nyugat-balkáni biztonsági közösség kialakulását, amely nem különálló biztonsági közösség, hanem az európai része.

A Nyugat-Balkánon az EU-politikák az állami elitnek címzettek, ami azt jelenti a biztonsági közösség szintjén, hogy annak embrionális formáját képviseli. Itt nem a közös identitás, hanem az elit együttműködése a meghatározó.[53] Az EU nyugat-balkáni politikái elősegítik a Deutsch által megfogalmazott feltételeket (fő értékek összeegyeztethetősége, politikai reagálás és viselkedés kölcsönös kiszámíthatósága), és azt, hogy a régió embrionális biztonsági közössége tovább fejlődjön. Az EU törekszik az általa közvetített értékek és modellek nyugat-balkáni elfogadottságára. A regionális döntéshozók az EU vívmányainak átvételével elkötelezik magukat ezen értékek mellett. A politikai reagálóképességet a kívülről kezdeményezett reformok érik el, amellyel elhozzák azokat a kompatibilis szabványokat, amelyekhez az államok igazodni tudnak. A konfliktus utáni környezetben kiemelt jelentőségűvé vált a biztonsági szektor reformja, amely intstitucionalista jellegével hozzájárult a biztonsági közösség fejlődéséhez. A viselkedés kiszámíthatósága pedig az intézmények megerősödésének eredményeként alakult ki.

Következtetés

A Nyugat-Balkánon a délszláv háborútól számított közel harminc év távlatából is elmondhatjuk, hogy továbbra is az államon belüli és az államközi dinamikát megoldatlan belpolitikai kérdések, két- és többoldalú viták jellemzik.[54] Ennek ellenére az európai biztonsági közösség pilléreként számontartott intézményi struktúrákhoz részben tagsági kapcsolatok révén már kötődnek. Az EU szerepe az európai béke és jólét elérésében megkerülhetetlen tényezővé vált. Az európai országok elkötelezettek a viták békés rendezése és a közös intézményeken keresztüli együttműködés mellett. Az EU segítségével a tekintélyelvű rezsimek stabil és dinamikus demokráciává változtak. Az EU 2003-as Európai Biztonsági Stratégiájában[55] megerősíti, hogy a Balkánnak az Európai Unióba való bekapcsolódást, stratégiai célt és reformösztönzést is kínál. E dokumentum normatív ereje különösen jelentős volt a reformok előmozdításában. A 2016-os Globális Stratégia[56] már számos negatív tendenciát tükröz a tágabb európai biztonsági környezetben. Hivatkozásokat tartalmaz a Nyugat-

[51] Uo. p. 95.
[52] Uo.
[53] Uo. pp.80-81.
[54] Jakesevic i. m.
[55] European Security Strategy, A Secure Europe in a Better World, (Európai Biztonsági Stratégia) 2003. https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf (Letöltés ideje: 2022. 05. 04.)
[56] The EU's Global Strategy (Globális Stratégia) 2016. https://www.europarl.europa.eu/RegData/etudes/ATAG/2016/579317/EPRS_ATA(2016)579317_EN.pdf (Letöltés ideje: 2022.05.04.)

Balkánra, mint EU-tagsági kilátásokkal rendelkező régióra, és továbbra is kulcsfontosságú átalakító hatalomnak tekinti magát a Nyugat-Balkán országaival szemben. A Nyugat-Balkán egy olyan régió, amelynek van egyértelmű csatlakozási perspektívája, bár jelenleg nincs terv az azonnali bővítésre. 2001 után az EU az egész régióban részt vett, és részt vesz bővítési programjával, valamint KBVP-politikája és missziói révén. A tagsághoz vezető feltételességi kritériumokat 2003-ban a Thessaloniki Csúcson fogalmazták[57] meg, azonban a KBVP-műveletekben történő részvétele a régiónak már 2002-ben a koppenhágai találkozón eldőlt. Ezt később a gyakorlatba is átültették az EUPM, az ALTHEA és a CONCORDIA missziók[58] által. Az EU nyugat-balkáni politikájának középpontjában kétségtelenül a regionális megközelítés áll,[59] amelyet az EU 2018-as hiteles bővítési stratégiájában is megerősített.[60] Természetesen a biztonság területén a NATO egy elengedhetetlenül fontos szervezet, azonban jelen esetben azért az EU a vezető biztonsági aktor, mert a NATO esetében hiányzik a regionális megközelítés, nem különösebben törekszik arra. Az idők során számos akadály maradt, amely a hazai fejlemények egymásra hatásának és az államközi vitáknak a következménye, amelyek az egész régió lassú fejlődését okozzák, és ezáltal a nyugat-balkáni országok az integrációs folyamat és felkészülés különböző szakaszában vannak.

A közelmúlt konfliktusa az okozója a nagyfokú bizalmatlanságnak, és emiatt inkább egy nagyobb európai struktúrába akarnak beilleszkedni, mintsem erősítsék a regionalizmust. Az 1990-es évek óta jellemző egy fentről lefelé irányuló megközelítés a regionális együttműködés helyett, és továbbra is létfontosságú a külső szereplők jelentősége a regionális dinamika és a regionális együttműködés fellendítésében. Mindezek mellett a politikai akarat hiánya hátráltatja a biztonsági együttműködés és a biztonsági közösség kiépítését.

Kérdések fogalmazhatóak meg ezen a ponton, hogy a regionális együttműködés jelenlegi szintje mennyiben elegendő a konfliktusok megelőzésére és a kétoldalú problémák megoldására, mindez pedig erőszak nélkül?

A Nyugat-Balkán jelenleg csak embrionális biztonsági közösséget képvisel, ami a biztonsági közösség kiépítésének legkorábbi szakasza. A külső szereplők tehát fontosak a biztonsági közösségi fázisok elitszintű interakcióinak előmozdításában. A közszintű biztonsági közösség fejlődése pedig sokkal kevésbé megfigyelhető. A regionális identitás nem jelenik meg egyértelműen a nyilvánosság szintjén. Nem

---

[57] The Thessaloniki agenda for the Western Balkans: Moving towards European integration; 2003.

[58] EUPM: rendőri misszió Bosznia-Hercegovinában, ALTHEA: katonai békefenntartó misszió Bosznia-Hercegovinában, CONCORDIA: békefenntartó misszió Észak-Macedóniában

[59] EMMERT, Frank – PETROVIC, Sinisa: The Past, Present, and Future of EU Enlargement; Fordham International Law Journal 2014/5. pp. 1349-1420. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2350&context=ilj (Letöltés ideje: 2022. 05. 04.)

[60] A credible enlargement perspective for and enhanced EU engagement with the Western Balkans, Strasbourg, 6.2.2018 COM(2018) 65 final; https://ec.europa.eu/info/sites/default/files/communication-credible-enlargement-perspective-western-balkans_en.pdf (Letöltés ideje: 2022. 05. 04.)

hihető az eddigi tapasztalok alapján, hogy az országok kormányai valódi kapcsolatot éreznek a térség többi országával.[61]

A külső szereplők és a hazai elit erőfeszítése ellenére az állapítható meg, hogy korlátozott előrelépés történt a biztonsági közösség kialakítása terén. A térség stabilizációs folyamatai még korántsem zárultak le, több hazai, regionális és a tágabb globális kihívás nemcsak a nyugat-balkáni országok viszonyát befolyásolja negatívan, hanem súlyosbítja a térség biztonsági összetettségét is, amely alapvetően nem stabil. Mindemellett fontos kérdésekben pedig nem is egyeznek a nyugat-balkáni országok álláspontjai az euroatlanti menetrenddel. Az egész régió szintjén hiányoznak olyan alapvetések, amelyeket Mohammed Ayoob[62] vagy Karl Deutsch fogalmaztak meg, ezáltal hiányzik a „mi" érzés, így a regionális együttműködés kialakítása nem tud szintet lépni a biztonsági közösség embrionális szakaszán túlmutató formái felé.

Felhasznált irodalom:

- A credible enlargement perspective for and enhanced EU engagement with the Western Balkans; Strasbourg, 6.2.2018 COM(2018) 65 final; https://ec.europa.eu/info/sites/default/files/communication-credible-enlargement-perspective-western-balkans_en.pdf (Letöltés ideje: 2022. 05. 04.)
- ACHARYA, Amitav: Collective identity and Conflict management in Southeast Asia; In: ADLER, Emanuel– BARNETT, Michael (eds.): Security Communities; Cambridge University Press, Cambridge, 1998.
- ACHARYA, Amitav: Constructing a Security Community in Southeast Asia: ASEAN and the Problem of Regional Order; Politics in Asia, Routledge, 2000.
- ADLER, Emanuel – BARNETT, Michael: Security Communities; Cambridge University Press, Cambridge, 1998.
- ARMSTRONG, Andrea – RUBIN, Barnett.: Policy Approaches to Regional Conflict Formations; Centre on International Cooperation, New York, 2002.
- AYOOB, Mohammed: Defining security: A subaltern realist perspective; In: KRAUSE, Keith – WILLIAMS, Michael C. (eds.): Critical Security Studies. Concepts and Cases, Routledge, 1997.
- BALOGH, István: Biztonságelméletek; Nemzet és Biztonság, 2013/3-4.
- BECHEV, Dimitar: Carrots, Sticks and Norms: the EU and Regional Cooperation in Southeast Europe; Journal of Southern Europe and the Balkans, 2006/1.
- BECHEV, Dimitar: Constructing South East Europe. Houndmills, Basingstoke, Hampshire; Palgrave Macmillan, 2011.

---

61 CRUISE, Rebecca J. – GRILLOT, Suzette R.: Regional Security Community in the Western Balkans. A Cross-Comparative Analysis; Journal of Regional Security 2013/1. pp.7-14.

62 AYOOB, Mohammed: Defining security: A subaltern realist perspective; In: KRAUSE, Keith – WILLIAMS, Michael C. (eds.): Critical Security Studies. Concepts and Cases, Routledge, 1997. pp. 121-146.

- BUZAN, Barry – WAEVER, Ole: Regions and Powers: The Structure of International Security; Cambridge University Press, Cambridge, 2003.
- CRUISE, Rebecca J. – GRILLOT, Suzette R.: Regional Security Community in the Western Balkans. A Cross-Comparative Analysis; Journal of Regional Security 2013/1.
- DEUTSCH, Karl Wolfgang: Political Community and the North American Area: International Organization in the Light of Historical Experience; Princeton University Press, Princeton, 1957.
- EMMERT, Frank – PETROVIC, Sinisa: The Past, Present, and Future of EU Enlargement; Fordham International Law Journal 2014/5. pp. 1349-1420. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2350&context=ilj (Letöltés ideje: 2022. 05. 04.)
- European Commission: The Stabilisation and Association process for Southeast Europe: First Annual Report; Brussels, COM(2002)163 final.
- European Security Strategy, A Secure Europe in a Better World, (Európai Biztonsági Stratégia) 2003. https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf (Letöltés ideje: 2022. 05. 04.)
- GLAURDIC, Josip: The Hour of Europe; Yale University Press, New Haven, Connecticut, 2011.
- GRILLOT, Suzette – D'ERMAN, Valerie J. – CRUISE, Rebecca J.: Developing Security Community in the Western Balkans: The Role of the EU and NATO Paper prepared for the EUSA; Tenth Biennial International Conference May 17-19, 2007. Montréal, QC, Canada Panel 1J: CSFP Case Studies; http://aei.pitt.edu/7789/1/cruise-r-01j.pdf (Letöltés ideje: 2022. 05. 02.)
- JAKESEVIC, Ruzica: Security Community Building In The Western Balkans – Wishful Thinking Or An Inevitable Future? Teorija In Praksa let. 56, 2019/1. https://www.fdv.uni-lj.si/docs/default-source/tip/vzpostavljanje-varnostne-skupnosti-na-zahodnem-balkanu-lepa-%C5%BEelja-ali-neogibna-prihodnost.pdf?sfvrsn=0 (Letöltés ideje: 2022. 05. 02.)
- JERVIS, Robert: Security regimes; International Organization, 1982/2.
- KALDOR, Mary: New and Old Wars; Polity Press, Cambridge, 2012.
- KAVALSKI, Emilian: Extending the European Security Community; Tauris, London, 2008.
- KOSCHUT, Simon: Regional order and peaceful change: Security communities as a via media in International Relations Theory. Cooperation and Conflict; Zeppelin University, Germany, 2014/4.
- MCCAUSLAND, Jeffrey: Arms control and the Dayton Accords; European Security, 1997/2.
- MILANOVIĆ, Jovana: Liberalizam I Bezbednosne Zajednice: Evropska Bezbednosna Zajednica Na Zapadnom Balkanu; Politicka revija, 2016/3.

- OSCE: OSCE Marks 20th Anniversary of Sub-Regional Arms Control Agreement, 2016. http://www.osce.org/cio/246991 (Letöltés ideje: 2022. 05. 03.)
- PUGH, Michael – COOPER, Neil – GOODHAND, Jonathan: War Economies in a Regional Context: Challenges of Transformation; Lynne Rienner, Boulder and London, 2004.
- REMEK, Éva: Az EBESZ – a biztonsági közösségépítés modellje; Budapest, Dialóg Campus Kiadó, 2018.
- RIDING, Alan: Conflict in Yugoslavia: Europeans Send High-Level Team; New York Times, 1991. http://www.nytimes.com/1991/06/29/world/conflict-in-yugoslavia-europeanssend-high-level-team.html (Letöltés ideje: 2022. 05. 02.)
- SHEENAN, Michael: International security; Lynne Rienner Publishers; Boulder, Colorado, 2005.
- SOLANA, Javier: Public Debate on Western Balkans. Intervention by High Representative of the Common Foreign and Security Policy to the General Affairs Council; Brussels, 2000. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/discours/gac%2010.7%20en.doc.html (Letöltés ideje: 2022. 05. 04.)
- STOJANVIC-GAJIC, Sonja – EJDUS, Philipp (eds.): Security Community Practices in the Western Balkans; Routledge, 2018.
- STRAZZARI, Francesco – COTICCHIA, Fabrizio: The Phantom Menace. Transnational Organized Crime and the Shaping of the Western Balkans; In: SOLIOZ, C.– STUBBS, P. (eds.): Towards Open Regionalism in South East Europe; Nomos Publishers, Baden-Baden, 2012.
- The EU's Global Strategy (Globális Stratégia) 2016. https://www.europarl.europa.eu/RegData/etudes/ATAG/2016/579317/EPRS_ATA(2016)579317_EN.pdf (Letöltés ideje: 2022.05.04.)
- VÄYRYNEN, Raimo: Stable Peace Through Security Communities? Step towards Theory-Building; University of Notre Dame, the Joan B. Kroc Institute For International Peace Studies. 2000.
- VUCETIC, Srdjan: The Stability Pact for South Eastern Europe as a Security Community-Building Institution; Southeast European Politics, 2001/2.
- WATANABE, Lisa: Securing Europe; Palgrave Macmillan, Houndmills, Basingstoke, Hampshire, 2010.
- WEAVER, Carol: Black Sea Regional Security: present multipolarity and future possibilities; European Security, 2011/1.
- The Thessaloniki agenda for the Western Balkans: Moving towards European integration; 2003.

DR. KASSAI KÁROLY

A HONVÉDELMI CÉLÚ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK SZÜKSÉGES MÉRTÉKŰ VÉDELMÉNEK BIZTOSÍTÁSA – GONDOLATOK EGY ZÖLD KÖNYV[1] SZÁMÁRA[2]

Bevezetés

Hazánkban a nemzetközi folyamatoknak megfelelően lépten-nyomon tapasztalható a kommunikációs szolgáltatások robbanásszerű fejlődése, a digitalizáció különböző szolgáltatásokban történő megjelenése, ami egyértelműen azonosítható tendencia a honvédelmi területen is.

A honvédelmi célú elektronikus információs szolgáltatások (vagy rendszerek) fejlődése, illetve a kapcsolódó védelmi kérdések nem tekinthetők új hadtudományi témának. A feszített ütemű szervezeti átalakulások, technikai fejlesztések kapcsán joggal felmerülhet a kérdés, hogy az elektronikus információs rendszerek üzemeltetését, elektronikus információbiztonságát, elektronikus információvédelmét,[3] illetve kibervédelmét biztosító keretrendszer pontosan illeszkedik-e a helyzethez? A jövőbeli várható változások, szervezeti és technikai korszerűsítési lépések igényelnek-e stratégiai szinten komolyabb korrekciós lépéseket? Felmerülhet-e hiányzó honvédelmi követelményeket, eljárásokat megfogalmazó stratégiai szintű – vagy alacsonyabb szintű – szabályozó hiánya?

E vizsgálat tehát nem napjaink egyik legnépszerűbb témájának – a kibervédelemnek – határait feszegeti, inkább gyakorlati szempontokra koncentrálva keresi a biztonsági szint megerősítéséhez és emeléséhez szükséges stratégiai szempontból kulcsfontosságú lépéseket.

A vizsgálat terjedelmi okok miatt nem tekinthető teljes körű feldolgozásnak, illetve tudatosan csak nyílt, publikusan megjeleníthető információkra támaszkodik, a következtetések során is csak ilyen információkat jelenít meg.

---

1 A „Zöld Könyv” kifejezés a stratégiai irányításról szóló jogszabály szerinti szakmai fogalmat takar, amelynek lényege a problémafeltárás és a megoldást segítő tényezők azonosítása.

2 A tanulmány Kassai Károly: A honvédelmi célú elektronikus információs rendszerek fejlesztéséhez szükséges továbblépés megalapozásához szükséges vizsgálat – egy zöld könyv kialakításának támogatása; Military and Intelligence Cybersecurity Research Paper 2022/5. munkájának felhasználásával illetve annak továbbfejlesztésével készült.

3 A két kifejezés alkalmazása nem csak a nyomatékosítást szolgálja: a hazai jogszabályi környezet a nem minősített adatkezelésre az „elektronikus információbiztonság”, míg minősített adatkezelés területén az „elektronikus információvédelem” kifejezést alkalmazza, amelyek mellett a kapcsolatrendszer és a tartalom részletes azonosítása nélkül – a nemzetközi trendnek megfelelően – megjelent a „kibervédelem” kifejezés is.

A hazai előzmények nagybani áttekintése

Magyarországon 2011-2012-ben már azonosítható a kibertérrel kapcsolatos kérdések nemzeti szintű kezelése. A nemzeti kibervédelmi feladatokról 2012-ben a Nemzeti Biztonsági Stratégia a 31. pontban rendelkezik.[4] Erre építve a Nemzeti Katonai Stratégia a Magyar Honvédség egyik céljaként jeleníti meg a hálózatalapú hadviselés feltételeinek megteremtését, és ennek részeként a Magyar Honvédség kibervédelmének megerősítését. A kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmak átfogó felülvizsgálatát és adott esetben módosítását.[5]

A 2013-as Nemzeti Kiberbiztonsági Stratégia meghatározza a kiberbiztonsági környezetet, kijelöli a nemzeti célokat és feladatokat, valamint megállapítja az eszközrendszert. A Stratégia a nemzetközi együttműködés vonatkozásában kiemeli, hogy Magyarország az atlanti együttműködést a kiberbiztonság terén kiemelten fontosnak tartja; az időközben kiadott NATO-nyilatkozatok[6] alapján ez azt is jelenti, hogy a kiberbiztonság kérdése a NATO Alapító Okmányának 5. cikkelye alá tartozó kollektív védelem körébe tartozik.[7]

A Stratégia mellett megjelent az állami és önkormányzati elektronikus információs rendszerekre vonatkozó elektronikus információbiztonsági követelményeket meghatározó törvény, és annak végrehajtási rendeletei.[8] A 2009 és 2010-ben csak minősített adatkezelésre koncentráló követelmények (törvény és végrehajtási rendeletek) így kiegészültek a nem minősített adatok védelmi kötelezettségeivel – az állami és önkormányzati elektronikus adatkezelésre szűkített hatállyal. Szentgráli Gergely 2013-as munkája részletesebben ábrázolja az akkori helyzetképet, amelyből *említésre érdemes elem az offenzív kibertér műveleti képesség fontossága*.[9]

2015-ben a szabályozási rend felülvizsgálaton esett át, és megjelent a manapság ismert szabályozási keret, azóta további változásokkal frissítve.

Ebben az időszakban a honvédelmi ágazatnál több vonalon történtek a honvédelmi elektronikus információs rendszerek biztonságát erősítő lépések. Technikai területen kicsit az előbb említett jogszabályok előtt, 2012-ben megjelent *a*

---

4 Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II.21.) Korm. határozat, 31. p.

5 Magyarország Nemzeti Katonai Stratégiájának elfogadásáról szóló 1656/2012. (XII. 20.) Korm. határozat 82., 33. pontok.

6 NATO Walesi Nyilatkozat, 2014. szeptember 05. (72. pont). NATO Varsói Nyilatkozat 2016. július 09. 71-72. pont

7 Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat 8. pont és 10. pont e) alpont.

8 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.) és a végrehajtására vonatkozó kormányrendeletek. Szakmai érdekesség, hogy a kidolgozás során folyamatosan a jogszabály kialakításán volt a hangsúly, a stratégiai megalapozás szükségessége gyakorlatilag a kiadás előtt, hirtelen jelent meg.

9 Az említett elem a 2021-es Nemzeti Katonai Stratégiában azonosítható. SZENTGÁLI Gergely: A magyar kibervédelem anatómiai képe; Felderítő Szemle, 2013. december, pp. 85-86. HU ISSN 1588-242X

honvédelmi elektronikus információbiztonság általános követelményeit meghatározó miniszteri utasítás,[10] kiegészítve a korábbi, szervezeti és szabályozási kereteket rögzítő Információbiztonsági Politikát.[11] Az akkor még jogszabályi követelmények nélkül megfogalmazott honvédelmi kontrollkészlet szabványalapú megközelítéssel, életciklus-szemléletet követve határozta meg a rendszerekre vonatkozóan az alapvető biztonsági szempontokat.

Az általános követelmények rendszerspecifikumaként 2013-ban az MH központi elektronikus információs rendszere biztonsági követelményeinek meghatározása érdekében a szakmai irányításért felelős szerv szakutasítást adott ki,[12] melynek legfontosabb feladata a hálózati struktúrához igazodva a felelősségi körök lehatárolása, illetve a helyi területi és központi szakfeladatok összehangolása, természetesen biztonsági szempontból.

A minősített elektronikus adatkezelés területén, NATO-kompatibilis módon, 2012-2014-ben megtörtént a rendszerek rendszerspecifikus biztonsági követelményekre,[13] a szabályozásra,[14] az ellenőrzésre[15] és az akkreditálási eljárásra[16] vonatkozó korszerű szempontrendszer meghatározása.

Napjainkban szakmaiságot nélkülöző nézet a rejtjelzés kibertértől függetlenül történő kezelése (és ezáltal biztonságosnak gondolva), így meg kell említeni ezen időszakban a katonai rejtjelzésre vonatkozó eljárásrend megújítását. 2013-ban hosszú egyeztetések és hatósági jóváhagyás után megtörtént az MH Rejtjelszabályzat kiadása.[17] A szakterületi kérdések összetettsége miatt a részleteket alacsonyabb szintű szabályozók jelentették meg 2014-ben.[18]

A helyzetet színesíti, hogy az 1996-ban kiadott, a minősített adatkezelési követelményeket meghatározó Általános Ügyviteli Szabályzat is tartalmaz

---

10 3/2012. (01. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról

11 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról. A politikáról részletesebb információk a következő publikációban olvashatók: KASSAI Károly: A honvédelmi tárca biztonságpolitikájában meghatározott követelmények, feladatok és azok fontosabb hatásai; Hadmérnök, 2009/4. pp. 183-190.

12 20/2013. (HK 12.) HVK HIICSF szakutasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszer-specifikus elektronikus biztonsági követelményeinek meghatározásáról

13 18/2016. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszerek Rendszer Biztonsági Követelményeire vonatkozó szabályokról

14 9/2012. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről

15 10/2012. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről

16 13/2016. (HK 7.) HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszerek biztonsági akkreditációs eljárásrendjéről

17 75/2013. (XII. 5.) HM utasítás a Magyar Honvédség Rejtjelszabályzat kiadásáról

18 Kassai Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban; Hadmérnök, 2015/3. p. 288.

elektronikus adatkezelésre (valamint rejtjelzésre) vonatkozó stratégiai szinten megfogalmazott elemeket.[19]

A kibertér védelmével kapcsolatos katonai érdekek azonosítása és szervezeti válaszok keresése a kormányzati stratégiák megjelenése előtt, 2011-ben kezdődött. Az alap- és teljes képesség kialakításának rendjére vonatkozó elrendelés honvédelmi miniszteri utasításban történt meg.[20] A szükséges szakfeladatokat 2013-ban miniszteri utasítás foglalta össze a Magyar Honvédség Kibervédelmi Szakmai Koncepció formájában,[21] *központi követelményként meghatározva a kibervédelmi fejlesztések keretét és a képességfejlesztési feladatokat*.

2013-ban a törvényi feladatszabás alapján a honvédelmi ágazati feladatok meghatározása érdekében honvédelmi miniszteri rendelet jelent meg,[22] kétéves időtartamra meghatározva a honvédelmi ágazati eseménykezelési és hatósági struktúrát. 2014-ben, az akkori szervezeti struktúrára alapozva megjelent a honvédelmi eseménykezelést szabályozó szakutasítás, az eljárások biztosítása, a működési rend kialakítása érdekében.[23] Folytatást jelentett az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (a továbbiakban: MH KCEHH) hálózati szintű elektronikus eseménykezelési feladatokat ellátó szervezeti elem kialakításának elrendelése HM utasítás formájában, 2015-ben.[24]

Az információbiztonsági területű lépések mellett a híradó, informatikai szakmai követelmények honvédelmi ágazaton belüli egységes megfogalmazása érdekében 2014-ben miniszteri utasítással elrendelve megjelent az MH Informatikai Szabályzat („ISZ").[25] A stratégiai híradó- és informatikai követelmények megfogalmazása megtörtént az MH Informatikai Stratégia („IS") kiadásával.[26]

2015-ben a Honvédelmi Szakpolitikai Program elektronikus információvédelmi/elektronikus információbiztonsági területen az MH és KNBSZ kibervédelmi képességek erősítését, a katonai szervezetek elektronikus minősített adatkezelésének fejlesztését, kapcsolódó feladatként a védelemigazgatási minősített adatkezelés és a tábori híradás fejlesztését tűzte ki célul.[27]

---

19 A többszörösen módosított HM-MH Titokvédelmi és Ügyviteli Szabályzat – Ált/3 (1996)

20 81/2011. (VII. 29.) HM utasítás a honvédelmi tárca Kibernetikai Védelmi Koncepció kialakításához szükséges feladatok meghatározásáról, 3. §. 5-6. p.

21 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról.

22 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről (hatályon kívül)

23 5/2014. HVK HIICSF szakutasítás a honvédelmi tárca elektronikus adatkezelő rendszerek incidenskezelési eljárásrendről

24 10/2015. (III. 26.) HM utasítás a Magyar Honvédség egyes szervezetei feladatrendszerének módosításával és vezetési rendszerét érintő átalakításokkal kapcsolatos egyes feladatokról, 3. § 1-2. p. (hatályon kívül)

25 39/2014. (V. 30.) HM utasítás a Magyar Honvédség Informatikai Szabályzatának kiadásáról

26 58/2014. (IX. 10.) HM utasítás a Magyar Honvédség Informatikai Stratégiájának kiadásáról

27 Honvédelmi Szakpolitikai Program 7.1, 7.2, 6.3 és 3.3 pontok.

Következő honvédelmi szakterületű változást jelentett 2016-ban egy kormányrendelettel elrendelt új követelmény,[28] amely szerint az ágazati elektronikus információbiztonsági hatósági felügyeleti feladatok a KNBSZ főigazgató hatáskörébe kerültek. Ugyanebben az évben megújult az először 2010-ben megkötött NATO-magyar kibervédelmi együttműködési megállapodás.[29]

Technikai síkon az akkori terminológia szerint híradó és informatikai (napjainkban infokommunikációs) fejlesztések gyorsítása érdekében 2015-ben kormányhatározat jelent meg,[30] ami jelzi, hogy az infrastruktúrafejlesztés keretén belül már vezetői szinten is érzékelhető a biztonsági feladatok, funkciók fontossága.

Az EU- és NATO-szintű hatások fokozódó adaptációja

Az EU-ban, 2017-ben, a szorosabb védelmi együttműködés egyik zálogaként megkezdődött az Állandó Strukturált Együttműködés,[31] ami kibervédelmi programokat is tartalmaz. Molnár Anna – Szabolcs Laura beszámolója szerint[32] a programok között szerepel a kiberfenyegetés és eseménykezelő információmegosztási platform, magyar részvétellel.[33] A többkörösen indított projektek következő csatlakozási pontja Kovács László 2020-as tájékoztatása szerint[34] hazánk csatlakozása a német kezdeményezésű Kiber- és Információs Műveleti Központ kialakítását célzó kezdeményezéshez.[35]

Az eljárások és technikai körülmények fejlődése 2017-2018 idején már többszörösen is érintette a honvédelmi ágazat különböző szakterületeit a nemzetközi kibervédelmi gyakorlatok, illetve a nemzetközi válságkezelési gyakorlatok kibervédelmi feladatainak megoldásában. A NATO Cyber Coalition és a NATO Kibervédelmi Kiválósági Központ[36] Locked Shield kibervédelmi gyakorlatsorozat,

---

[28] 22/2016. (II. 17.) 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 szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról, 1. §.

[29] Hungary signs new MoU on cyber defence cooperation; https://nicp.nato.int/hungary-signs-new-mou-on-cyber-defence-cooperation/index.html (Letöltés ideje: 2022. 06. 10.)

[30] 1500/2015. (VII. 23.) Korm. határozat a Magyar Honvédség kibervédelem szempontjából kiemelt jelentőségű komplex informatikai fejlesztéseihez kapcsolódó beszerzéseknek a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló 228/2004. (VII. 30.) Korm. rendelet 2. § (3) bekezdés d) pontja szerinti minősítéséről, 1. p.

[31] Permanent Structured Cooperation (PESCO).

[32] Molnár Anna – Szabolcs Laura: Megerősített együttműködés, változó geometria. PESCO; Hadtudomány 2020/4. p. 87-88.

[33] A kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform.

[34] Magyarország élen jár az európai katonai kibervédelemben; https://honvedelem.hu/hirek/magyarorszag-elen-jar-az-europai-katonai-kibervedelemben.html (Letöltés ideje: 2022. 06. 10.)

[35] CIDC: Cyber and Information Domain Centre

[36] NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE

illetve a NATO és nemzeti erőket is alkalmazó válságkezelési gyakorlatsorozat kibervédelmi forgatókönyvei[37] évről-évre újabb, technikai és jogi, hadműveleti szempontból bonyolultabb feladatokat szabnak a végrehajtó, üzemeltető, kibervédelmi és egyéb szakterületű állománynak. A Locked Shield gyakorlatsorozat evolúciója jól mutatja a kibertér kezeléséhez szükséges eszközök és megoldások számának növekedését. A kezdetben tudatosan technikai orientációjú gyakorlat napjainkban már csak részeiben ismerhető fel. A különböző forgatókönyvek megoldásához továbbra is magas szintű technikai megoldó képesség és külső-belső együttműködési lépés szükséges, amelyet napjainkban már védelemigazgatási és válságkezelési, hadműveleti szakértőkből álló stratégiai csoporttal, jogi tanácsadó csoporttal, média- és stratégiai kommunikációs támogatással megerősítve lehet csak sikeresen végrehajtani.

Az említett NATO-alapú tevékenységek mellett említést érdemel a Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet által szervezett első nemzeti kibervédelmi gyakorlat lebonyolítása 2019. decemberben.[38]

Az EU katonai ambíciószint emelkedését jelzi a 2021. februárban[39] és júniusban[40] lezajlott első kétfokozatú, katonai eseménykezelő központoknak rendezett kibervédelmi gyakorlat.

A 2021. októberben lebonyolított hibrid műveleti fókuszú „Létfontosságú Védőbástya 2021" nemzeti válságkezelési gyakorlat is tartalmazott kibervédelmi feladatsort.[41]

Ezek a történések tanúsítják, hogy nagyobb publicitás nélkül megkezdődött a polgári és a honvédelmi, katonai nemzetbiztonsági feladatokon belül a kibervédelmi kérdések gyakorlati szintű kezelése.

A napi életben és a gyakorlatokon megoldandó technikai feladatok elsajátítása hosszú és rögös utat jelent az érintett állománynak, ahol egy lehetséges megoldás a NATO Kibervédelmi Központ által biztosított tanfolyami képzési lehetőség, amelyet

---

37 NATO Crysis Management Exercise – NATO CMX

38 Sikeresen lezajlott a magyar kiberbiztonsági gyakorlat (HunEx2019); https://nki.gov.hu/intezet/kozlemenyek/sikeresen-lezajlott-a-magyar-kiberbiztonsagi-gyakorlat (Letöltés ideje: 2022. 06. 10.)

39 Cyber defence exercise brings together military CERTs; https://eda.europa.eu/news-and-events/news/2021/02/19/cyber-defence-exercise-brings-together-military-certs (Letöltés ideje: 2022. 06. 10.)

40 EDA MilCERT Interoperability Conference talks strategy https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy (Letöltés ideje: 2022. 06. 10.)

41 A gyakorlat során cél volt a katonai, rendvédelmi és civil képességek összehangolt tevékenységének gyakoroltatása a létfontosságú létesítményeket veszélyeztető hibrid fenyegetések és támadások elleni fellépés időszakában. 30/2021. (VII. 23.) HM utasítás a „Létfontosságú Védőbástya 2021" nemzeti létfontosságú rendszerelemeket érintő válságkezelési gyakorlat honvédelmi ágazatot érintő feladatainak előkészítéséről és végrehajtásáról, 2 §. (3) bek.

esetenként kihelyezett tanfolyammal is lehet biztosítani, mint 2016-ban ez megtörtént a Nemzeti Közszolgálati Egyetem biztosításában.[42]

2017-ben a jogszabályok szerinti eseménykezelésre, sérülékenységvizsgálatra és hatósági feladatokra vonatkozó ágazati követelmények részletes meghatározása érdekében HM-utasítás jelent meg.[43]

A 2016-os NATO-követelményekkel összhangban a magyar honvédelmi szabályozás jogszabályi változásokkal korszerűsödött. A Hvt. 2018-as módosításában megjelent a Honvédség feladatai között a kibertér védelme, illetve ezzel kapcsolatban a szövetségesi, nemzetközi együttműködési kötelezettség. Meghatározott esetekben a Honvédség felhasználható a kibertérből érkező és egyéb elektronikai fenyegetések elhárításában, illetve a NATO-, EU-megoldásnak megfelelően a törvény is leszögezte, hogy a kibertér műveleti területként kezelendő. Új feladatként jelent meg a „honvédelmi veszélyhelyzet" fogalom, amikor a Kormány elrendelheti a KNBSZ és a honvédségi szervezetek felderítő, elhárító, valamint kibertér-műveleti erők tevékenységeinek fokozását.[44]

2019-ben folytatódtak a változások. A Hvt. megalapozta, hogy a Honvédség műveleteinek támogatása érdekében nyújtott kibertér-műveleti támogatáshoz a Honvédség eszközei szabályozottan átengedhetőek a KNBSZ számára. Megjelentek a katonai kibertér-műveletekre vonatkozó különös szabályok (eljárásrend, a kibervédelmi ügyeletes parancsnok feladatköre). [45]

2019-ben változott továbbá a nemzetbiztonságról szóló törvény (Nbtv.), ahol a KNBSZ eddigi, a kibertevékenységekről történő információgyűjtési feladata bővült a honvédelmi ágazati elektronikus információbiztonsági feladatok ellátásával, illetve a minisztérium és a Magyar Honvédség Parancsnoksága információvédelmi tervező munkához szükséges információk biztosításával. A KNBSZ kibertér-műveleti képességeivel ellátja honvédelmi érdekek nemzetbiztonsági jellegű védelmét és támogatja a MH kibervédelmét és műveleteit.[46]

2019-ben stratégiai szintű, lényegi szervezeti változás a Honvédelmi Minisztérium és Magyar Honvédség Parancsnoksága szervezetek elkülönülése (dezintegráció). Ennek a lépésnek szakmai vonzata a korábban is vezérkari csoportfőnökség által végzett híradó, informatikai és információvédelmi szakmai irányítói hatáskör megjelenése mellett a kibervédelmi területű haderőnemi

---

[42] Átfogó képet kaptak a kibertér védelméhez szükséges módszerekről és eszközökről; https://honvedelem.hu/hirek/hazai-hirek/atfogo-kepet-kaptak-a-kiberter-vedelmehez-szukseges-modszerekrol-es-eszkozokrol.html (Letöltés ideje: 2022. 06. 10.)

[43] 15/2017. (IV. 28.) HM utasítás a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól. 2020-ban megtörtént a bekövetkezett változások követése, így ez a szabályozás pontosítottnak tekinthető.

[44] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, 36. § (2) g. pont, 80. §. 5 és 22. pont, 21. § A (1) d. pont. (Módosítás: a 2018. évi CX. törvény szerint.)

[45] Hvt. 37. §. (5) d. pont, 62/A (1-8).

[46] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (módosítás: 2019. évi CV. Törvény) 6. §. f, g. pontok

szemlélőség megjelenése, a stratégiai szintű szakfeladatok (tanácsadás, fejlesztési feladatok irányítása, kommunikációs feladatok) biztosítása érdekében.

2019-ben Szentendrén megtörtént a Kiberakadémia megnyitója, újabb támogatási lehetőséget nyújtva a képzési lehetőségek között.[47] 2021 szeptemberében már folytak a Kiberműveleti Központ Előkészítő Osztály tanfolyamai, a hivatkozott forrás szerint – más tanfolyamok mellett – egynapos kibervédelmi tudatossági tanfolyamok is zajlottak.[48]

A katonai elektronikus információbiztonságra fókuszáló képzés keretei korábban, 2005-2006 környékén alakultak a Nemzeti Közszolgálati Egyetem jogelődjénél, egy korábbi cikk beszámolója szerint. Ekkor alakult ki a rendszerbiztonsági felelős (később felügyelő) és a rendszeradminisztrátori biztonsági képzési tematika, az elektronikus információvédelmi kockázatelemző és a kompromittáló kisugárzás elleni védelmi szaktanfolyamok, valamint a rejtjelző alaptanfolyamok, eszközkezelő tanfolyamok rendje.[49]

Szabályozási és doktrinális kérdések

2020-ban új NATO-követelményként azonosítható a NATO Kibertér-műveleti Doktrína megjelenése,[50] amelynek ratifikálása miniszteri utasítás formájában hazánkban is megtörtént.[51]

A NATO-doktrína ratifikálása mellett saját nemzeti követelményként miniszteri feladatszabásban szereplő feladat[52] a nemzeti kibervédelmi doktrína kiadása.[53] A szervezetkialakításra vonatkozó folyamat felgyorsulását (a gondolkodás irányának változását) jelzi, hogy a műveleti alapokat meghatározó doktrína kiadása előtt megjelent a Kiber- és Információs Műveleti Központ 2022-es megalakítását elrendelő

---

47 Átadták a Magyar Honvédség Kiber Képzési Központját; https://honvedelem.hu/media/aktualis-videok/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat.html (Letöltés ideje: 2022. 06. 10.)

48 Fókuszban a kiberbiztonság (2021. 09. 17), https://honvedelem.hu/hirek/fokuszban-a-kiberbiztonsag.html (Letöltés ideje: 2022. 06. 10.)

49 Kassai Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban; Hadmérnök, 2015/3. p. 282.

50 NATO Cyber Operations Doctrine – AJP 3.20. (2020)

51 42/2020. HM utasítás egyes NATO egységesítési jelzések elfogadásáról, 5. §.

52 14/2021. (III. 19.) HM utasítás a honvédelmi szervezet 2021. évi kiemelt feladatainak, valamint a 2022–2023. évi fő célkitűzéseinek meghatározásáról. Az éves fő feladatokat meghatározó miniszteri feladatszabás részletes szakmai követelményeket egy szakterületen sem határoz meg, így a nemzeti doktrínára vonatkozó elvárások itt nem azonosíthatók. Az úttörő jellegű doktrína kidolgozási folyamat mellett megemlítendő, hogy a korábbi kiadású Összhaderőnemi Doktrína, a Hadműveleti Doktrína, az Információs Műveletek Doktrína, a HÍD terminológiában, a műveleti folyamatokban nem követi az új gondolatokat, mely helyzet sürgős összehangolási feladatok szükségességét jelezi.

53 A Doktrína kiadása 2022. 05.02-én megtörtént: 175/2022. (HK 4.) MH PK intézkedés a Magyar Honvédség Kibertér műveleti doktrína (1. kiadás) című szolgálati könyv kiadásáról

miniszteri szervezési utasítás, ami tartalmi eltérést mutat a korábbi, kibervédelmet célzó feladatkörhöz képest.[54]

A kibertérre vonatkozó doktrinális kérdéseket nem lehet önállóan, az összhaderőnemi és a többi funkcionális doktrína figyelembevétele nélkül megoldani. Így figyelmet igényel a kibertér-kérdések összhangjának megteremtése:

- A 2018-ban kiadott MH Összhaderőnemi Doktrínával,[55] amihez kapcsolódó feladatot jelenthetnek a korábban említett jogszabályi változások, és a 2020-as új Nemzeti Katonai Stratégiában megjelenő kibertér-feladatok.
- A 2014-ben kiadott MH Információs Műveleti Doktrínával – ahol az elmúlt időszak változásainak megfelelően pontosan ki kell dolgozni az információs műveletek folyamatainak és eljárásainak lényegi elemeit, a korábban említett, megalakítás előtt álló szervezeti elem működésének biztosítása érdekében – biztosítani kell a katonai műveletek sikeréhez szükséges információs műveletek integrálását a műveleti tervezés és végrehajtás folyamataiba.
- A 2013-ban kiadott MH Összhaderőnemi Híradó- és Informatikai Doktrínával, tekintettel arra, hogy a kibertér-műveletek tervezése és végrehajtása során a híradó és informatikai infrastruktúra megkerülhetetlen.[56] Ennél a kérdésnél még meg kell oldani a korábban említett MH Informatikai Szabályzattal és az MH Informatikai Stratégiával történő összehangolási feladatokat is.

A doktrinális kérdésekkel foglalkozó Mező Andrástól markáns megfogalmazásban olvasható 2018-ban, hogy *„… a szabványos NATO-doktrínákon nyugvó magyar katonai gondolkodás Magyarország biztonságának egyik alapvető pillére.”*,[57] ami jelzi, hogy a doktrínák kialakítása és pontosítása, valamint tartalmi összehangolásuk fontos eleme kell, hogy legyen a katonai kultúrának.

A katonai műveletek tervezése és végrehajtása nem csak az irányelveket jelző doktrínák, hanem részletesebb követelményeket meghatározó szabályozók kérdése is. A NATO átfogó művelettervezési irányelveire[58] építve 2013-ban megjelent az MH Törzsszolgálati Utasítás, amelynek feladata a katonai műveletek tervezéséhez és végrehajtásához, irányításához szükséges összes folyamat, feladat, felelősség és kapcsolódási pontok meghatározása, ami biztosítja a Honvédség – mint gépezet – működését önállóan, vagy szövetségi keretekbe ágyazva. A NATO-követelmények

---

54 32/2021. (VII. 23.) HM utasítás a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról

55 Hatályba léptette: 462/2017. (HK 12.) HVKF szakutasítás.

56 A nyilvánvaló összefüggést jelzi a NATO doktrína értelmezése, mely szerint a híradó és informatikai infrastruktúra műveletek kibertér műveletnek minősülnek a védelmi, offenzív és felderítő műveletek mellett.

57 A gondolat folytatása: „A doktrinális gondolkodás elhanyagolása megfosztaná a hadsereget a módszeres gondolkodástól, a szövetségi együttműködés lehetőségétől, a haderő konzisztens fejlesztésétől.” MEZŐ András: A Magyar Honvédség doktrínafejlesztése – 2. rész, Hadtudomány, 2018/1. p. 55.

58 Allied Command Operations: Comprehensive Operations Planning Directive (COPD INTERIM V2.0), 2013 (hatálytalan). Jelenleg az irányelv 2021-ben kiadott harmadik változata van érvényben.

változtak 2021-ben, az új tervezési irányelvek megjelenésével számos ponton kibertér-műveleti szempontok jelentek meg. Emiatt kifejezetten kibertér-műveleti síkra egyszerűsítve is igényként jelentkezik az Utasítás modernizálásának kérdése.

A szabályozottsággal kapcsolatos részletes értékelést ez a tanulmány nem vállalhat, egyrészt a téma érzékenysége, másrészt a teljes körű, részletes vizsgálat hiánya miatt. A működéshez szükséges folyamatokra, feladatokra és felelősségekre vonatkozó szabályozási kérdések fontosságának megítélése, a stratégiai súly érzékeltetése Farkas Ádám 2021-es írásában szemléletesen olvasható. Eszerint: *„Minden jól strukturált és felkészült védelmi szervezet számára alapvető fontosságú a szabályozottság, hiszen előre meghatározott protokollok nélkül nincs hierarchia, (…) további veszélyre figyelmeztető gondolat, hogy „ha a védelmi és biztonsági funkciók szabályozása nem kellően korszerű, nem kellően konzisztens, nem kellően stabil és kiszámítható, akkor az az állammal szembeni bizalom erózióját eredményezheti.”*[59] Ezek a gondolatok megvilágítják, hogy ***a folyamatok (vagy katonai műveletek) szabályozása nem rosszul értelmezett bürokratikus útvesztő, hanem nélkülözhetetlen, mással nem pótolható, vezetéssel szemben támasztott követelmény.***

Jelen vizsgálat nem csak a szabályozási kérdések vizsgálatát célozza, így elégséges csak rámutatni, hogy a hadtudományi publikációkban már megkezdődött a szabályozási, államszervezési kapcsolódások kérdéseinek vizsgálata.[60]

Ezek a vizsgálatok az elektronikus információbiztonság (vagy kiberbiztonság) kereteinél lényegesen szélesebb körűek, de egyben jelzik, hogy ezeket a kérdéseket komolyabb vizsgálatokkal kell támogatni, illetve a normál életben e szabályozási kérdésekre lényegesen nagyobb hangsúlyt kell fektetni.

Ez a gondolkodás segíthet új megoldásában különösen azzal kapcsolatban, hogy milyen logikai kapcsolódást kell kialakítani a jogszabályok és a katonai szabályzatok között, hogyan kapcsolódik a doktrinális rend az egyéb szabályozási kérdésekhez (szükséges-e a magyar katonai doktrínák publikus változatainak kiadása a láthatóság és hitelesség támogatása érdekében), illetve a NATO és EU katonai politikák (policy), stratégiák, direktívák és irányelvek hogyan kerülnek át a nemzeti szabályozási körbe.

Esetenként felbukkanó, markánsan fogalmazó, a katonai képességfejlesztés fontosságát tükröző vélekedések szerint nem jogszabályokra, szabályozásra van szükség, hanem cselekvésre! Ez a populáris megközelítés a köznapi életben

---

[59] FARKAS Ádám: A kortárs technikai-fejlődés és innováció viszonya a honvédelmi szabályozással, MTA Law Working Papers, ISSN 2064-4515, 2021/4, p. 3, 5.

[60] FARKAS Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán; Military and Intelligence Cyber Security Research Paper 2021/1; VIKMAN László: A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására; Military and Intelligence Cyber Security Research Paper 2021/2.; SPITZER Jenő: A francia kibervédelmi és kiberbiztonsági rendszer egyes stratégiai aspektusai; Military and Intelligence Cyber Security Research Paper 2021/3; KELEMEN Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése; Military and Intelligence Cyber Security Research Paper, 2022/1.

szimpatikus, haladáspártinak könyvelhető, ugyanakkor elfedi az előbbi gondolatot a honvédelmi területen a szabályozottság fontosságáról. Ugyanilyen népszerű, gyakran bemutatott nézet a kibertérben történő helyzetek villanásnyi idő alatt történő bekövetkezése („nincs idő jogértelmezésre, azonnal kell cselekedni"), illetve visszatérő jellegű még a kibertér „határtalansága" (az adatok és szolgáltatások „nem az országhatárok szerint működnek") és a történések megítélésének nehézsége. A hasonló, kibertéri feladatokat népszerűsítő, bár kevésbé szakszerű gondolatok ellenszere csak a tanulás lehet! Szükség van annak megértésére, hogy ***a villámlásszerűen történő események a valóságban hosszú előkészítés eredményei*** (ahol meg kell találni a detektálási lehetőségeket), illetve *a* ***„légiesnek" tűnő adatmozgások hardver- és szoftverelemekhez köthetők, ami egyben földrajzi kötődést is kell, hogy jelentsen*** (még akkor is, ha egy világűrben keringő objektumról, vagy nyílt óceánon tartózkodó hajóról van szó).

Vasvári Géza 2018-as szakmai szintet célzó írásában erre vonatkozóan összefoglalóan megjegyezte, hogy hazánk NATO-csatlakozása óta a jogszabályi környezet jelentősen átalakult, fejlődött. A digitalizáció (és az egyéb technikai fejlődés) újabb kihívásokat eredményez *„ami megköveteli a szabályozási környezetnek az elért eredmények és az információbiztonsági trendek elemzésén alapuló folyamatos felülvizsgálatát"*.[61]

Gerőfi Szilárd 2017-es, az utolsó évtizedre fókuszáló írása szerint a híradó szolgálat fejlődése lehetővé tette a katonai informatikai rendszerek látványos bővülését. A két szolgálat (szakterület) a vizsgált időszakban jelentősen közelített egymáshoz, szorosan együttműködik, amelyhez csatlakozik az elektronikus információvédelem is. Más helyen megállapítja, hogy az informatika területén is időről-időre változott az irányításra vonatkozó elképzelés (centralizálás vagy decentralizálás), illetve az elektronikus információvédelem is „sokáig kereste helyét a struktúrában", ami jelzi, hogy a fejlődés nem minden esetben zökkenőmentes lépésekből állt e szakterületeknél. Emellett további idézésre érdemes a szakállomány biztosításával és megtartásával kapcsolatos nehézség a polgári szféra elszívó ereje miatt.[62]
Ez az inkább szervezeti oldalú vizsgálat érdemi magyarázattal szolgálhat a rendszerek (szolgáltatások) irányításával és szabályozásával kapcsolatos összetett helyzetre.[63]

Új nemzetközi jelenség az elrettentés (deterrence) összetett feladatrendszerének a kibertérben történő kiemelése és a „kiber (kibertér) -elrettentés" gondolatkör kialakítása, fejlesztése. A kérdés helyes megoldása nem lehet e vizsgálat tárgya, így csak annyit célszerű rögzíteni, hogy az elrettentés komplex logikájának megértése nagy segítséget nyújthat az új, stratégiai szintű gondolatok formálásához. Ennek része kell, hogy legyen annak megítélése, hogy ***milyen meglévő, reális képesség, folyamat, feladatrendszer tekinthető hitelesnek, működőképesnek, ezáltal mások által is***

---

[61] VASVÁRI Géza: a katonai szervezetek elektronikus információvédelmi képességeinek fejlesztésével kapcsolatos feladatok, Hadtudományi Szemle, 2018/5. pp. 73-89. p. 87.

[62] GERŐFI Szilárd: A Magyar Honvédség vezetéstámogató rendszere alkalmazásának lehetőségei a XXI. századi kihívások tükrében; Hadtudomány, 2017/3-4. p. 97, 103.

[63] Megjegyzendő, hogy más minisztériumokban a Gerőfi által szemléltetett folyamat helyett szervezeti elkülönítésen alapuló kultúrák alakultak ki és az elektronikus információvédelem (benne: rejtjelzés) és elektronikus információbiztonság a távközléstől (vagy infokommunikációtól) független szervezeti elemként dolgozik (pld. Biztonsági Főosztály).

elrettentőnek*.** Hasonló kategória kell, hogy legyen a NATO- és EU-követelményekből lebontandó ***ellenállóképesség (resilience),[64] ***ahol nem csak alrendszer-, rendszerszintű, hanem nemzeti, ágazatokon átívelő, illetve nemzetközi szektorok közötti civil–katonai képességek összehangolását kell célul kitűzni,*** beleértve természetesen a digitalizációs megoldásokat, kibertér-műveleti kérdéseket.

Az eddigiekben bemutatott szervezeti, technikai és eljárási lépések mellett *nem elhanyagolható a humán faktorban rejlő kockázatok tudatos ellensúlyozása*. A honvédelmi ágazatnál a biztonságtudatosítás keretén belül több lépéssel, fokozatosan kialakult a felhasználók támogatása érdekében kialakított, elektronikus közlemények formájában megvalósított – a kibervédelmi kockázatok csökkentését célzó tájékoztatási rendszer –, amelyet a 2020-as Covid19 veszélyhelyzet a gyakorlatban tesztelt Knapp Gábor tájékoztatása szerint.[65] A tudatosítás formavilága változatos, mint azt egy korábbi beszámoló is mutatja. 2010-ben az akkori Zrínyi Miklós Nemzetvédelmi Egyetem, Híradó Tanszék és a HM Honvéd Vezérkar Híradó és Informatikai Csoportfőnökség, Elektronikus Információvédelmi Osztály közösen megszervezte az első Katonai Elektronikus Információvédelmi Konferenciát. Az éves ismétlődésű – mai napig zajló – rendezvénysorozat célja a szakmai konzultáció és tapasztalatcsere.[66] A 2022. májusi konferencián a közönség meghallgathatta Magyarország kiberkoordinátorának bevezető előadását a készülő nemzeti kiberbiztosági stratégiáról, információk hangzottak el a kiberműveleti doktrína legfontosabb kérdéseiről, illetve a Kibervédelmi Akadémia által is biztosított képzési lehetőségekről. [67]

Remélhetően ehhez hasonló gyakorlat alakul ki az EU Kibervédelmi Hónap rendezvénynaptárában megjelenő, a Katonai Nemzetbiztonsági Szolgálat által szervezett 2021-es szakmai konferencia nyomvonalán. A konferencián Knapp Gábor az eseménykezelés vonalán – korábbi publikációjával összhangban – a minősített adatkezelésre jogosított rendszerek, illetve a rejtjeltevékenység sajátosságait vizsgálta, és rámutatott, hogy ebben a speciális üzemeltetési környezetben sem kizárható incidensek bekövetkezése, és az azok kezelésére vonatkozó megoldások kialakítása és fenntartása. Farkas Ádám jelezte, hogy az állami funkciókat összehangoltan, hibrid környezethez igazodó szemlélettel kell kialakítani. Marsi Tamás az államigazgatásban bevezetett korai előrejelző rendszer kapcsán az incidenskezelés támogatására, és a reagálási idő csökkentésére mutatva jelezte ennek a védelmi vonalnak a fontosságát. Király Ágnes a kibertérfenyegetettség-elemzés (Cyber Threat Intelligence – CTI) lényegi ismertetésénél a strukturált megközelítés fontosságára hívta fel a figyelmet (stratégiai, hadműveleti és harcászati (taktikai), illetve rámutatott, hogy az általánosan ismert életciklus-modellt (szemléletet) – a

---

64 Akár az elrettentés gondolatához is köthetően.

65 KNAPP Gábor: Az elektronikus információbiztonság- tudatosítás feladatrendszerének honvédelmi ágazati szempontú vizsgálata és kihívásai; Szakmai Szemle XVIII. évfolyam 3. szám, p. 150, 154.

66 KASSAI Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban; Hadmérnök 2015/3. p. 282.

67 Nemzetközi Katonai Információbiztonsági Konferencia (2022. 05. 03.); https://honvedelem.hu/hirek/nemzetkozi-katonai-informaciobiztonsagi-konferencia.html (Letöltés ideje: 2022. 06. 10.)

fennálló nehézségek mellett – ezen a területen is alkalmazni kell.[68] A szakmai konferenciák vonalától eltérő, de hasonlóan fontos terület a szakértői szintű együttműködés. Ennek szükségességére mutat rá a V4-országok katonai kibervédelmi szervezeteinek 2021 szeptemberében lebonyolított találkozója a Magyar Honvédség Parancsnokságának kibervédelmi haderőnemi szemlélőjének szervezésében. A már említett német vezetésű CIDCC PESCO-projekt magas szintű képviselője is részt vett a rendezvényen, bemutatva a projekt legfontosabb jellemzőit.[69]

Egy újabb kiberszakterületi dimenzióra mutat rá az MH Kiber- és Információs Műveleti Központ által fenntartott „Kibertudatosság" oldal, rövid, statikusabb figyelmeztetést, figyelemfelkeltést sugározva az olvasók felé célzott címek mentén, mint pld. adatvédelem, veszélyforrások, pszichológiai manipuláció stb.[70]

A fontosabb történések lezárásaként említendő a Nemzeti Katonai Stratégia 2021-es kiadása,[71] amiben már a kibertérben zajló honvédelmi érdekérvényesítés több eleme is olvasható.

2021-es további változás a nemzeti felügyeleti rendben, hogy a megújuló Nemzeti Kiberbiztonsági Koordinációs Tanács munkájában állandó tagként részt vesz a KNBSZ főigazgatója is.[72]

Honvédelmi területen irányadónak kell tekinteni az éves miniszteri feladatszabást. Ennek értelmében 2022-ben kiemelt szakfeladat a honvédelmi ágazati elektronikus eseménykezelés, sérülékenységvizsgálat és a hatósági felügyeleti funkciók területén a képességfejlesztés folytatása, valamint a Magyar Honvédség Kiber- és Információs Műveleti Központ megalakítása, majd kezdeti műveleti képességének elérése 2024 végére.[73]

Utolsó gondolatként célszerű utalni a már látható, érzékelhető kibertér-kihívásokra, amelyek kezelése már a közeljövőben is megoldandó feladatokat jelenthet.

A nemzeti szuverenitás biztosítása, a szükséges önvédelmi lépések megtétele nem képzelhető el a betudás (attribúció) témakörének feldolgozása, az eszkalációs folyamatok kialakítása vagy a szükséges feladatok gyakoroltatása nélkül. Páll-Orosz Piroska 2021-es írása szerint ***szükség van – más nemzetekhez hasonló módon – a betudásra vonatkozó nemzeti álláspont megfogalmazására és kinyílvánítására,***

---

68 MAGYAR Sándor: Katonai kibertér 2021. Konferencia beszámoló; Szakmai Szemle 2021/4. p. 138, 146, 147.

69 A visegrádi országok katonai kibervezetői tanácskoztak Budapesten (2021. 11. 15.), https://honvedelem.hu/hirek/a-visegradi-orszagok-katonai-kibervezetoi-tanacskoztak-budapesten.html (Letöltés ideje: 2022. 06. 10.

70 http://tavoktatas.mil.hu/tudatossag/rolunk/index.html; 2022. (Letöltés ideje: 2022. 06. 10.)

71 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

72 259/2021. (V. 20.) Korm. rendelet a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról, 26. §. (3) bek.

73 3/2022. (I. 27.) HM utasítás a honvédelmi szervezet 2022. évi kiemelt feladatainak, valamint a 2023-2024. évi fő célkitűzéseinek meghatározásáról; 2. §. 47, 56. p. és 3. §. 31. p.

illetve ezzel párhuzamosan a sikeres azonosításhoz szükséges összes szereplő feladatainak azonosítására és tevékenységük összehangolására.[74]

A korábbi megállapítások mutatják, hogy jogszabályokban, nemzeti stratégiákban már megjelennek a kibertér-műveleti offenzív lehetőségek. Kovács László 2021-es írásában ezt a feladatot kezdte tanulmányozni, több helyen is aláhúzva ***a terminológiai feszültséget, az eltérő megközelítések ütköztetésének szükségességét, illetve elkezdte a hibrid műveleteken belül értelmezendő offenzív műveletek fontosabb elemeinek azonosítását,*** mint a szélesen értelmezett felderítés és adatgyűjtés, a támadás és a hatáselemzés.[75]

A helyzetkép értékelése

A fenti, lényegi kérdéseket célzó áttekintés megalapoz néhány alapvető felismerést, ami segíthet a honvédelem érdekében szükséges kiberbiztonsági szakfeladatok továbbgondolása érdekében:

- Az utolsó 10 évben igazolható, hogy nemzeti szinten jelentős lépések történtek az elektronikus információs rendszerek védelmének erősítése érdekében (pl. felelősség kijelölése, szervezeti és technikai követelmények, hatósági szakfeladatok, képzési követelmények). A nemzeti követelmények között a honvédelmi tárcára vonatkozó követelmények egyértelműen azonosíthatók, illetve a kormányzati szintű felelősségek vagy az azokban történő változások (pl. minősített adatkezelés, létfontosságú infrastruktúra védelem, adatvédelmi felügyelet) jól követhetők.
- A honvédelmi célú elektronikus információs rendszerek üzemeltetésére és biztonságára az évezred kezdetétől számos szabályozó, különböző szinten határoz meg felelősségeket, eljárásokat és feladatokat minősített és nem minősített adatkezelés esetén egyaránt, melyek naprakészsége, illetve összehangoltságuk kérdése nehezen megítélhető.
    - A honvédelmi ágazaton belüli egységes megfogalmazású, érvényben lévő elektronikus információbiztonsági, információvédelmi és kibervédelmi keretrendszer nem azonosítható. A felelősségek, követelmények, folyamatok és feladatok meghatározása stratégiai szinten nem összehangolt és egységes, melynek következményeképpen az egyes alsóbb szintű szabályozók, követelmények sem összehangoltak. Emiatt az alkalmazó szervezetek, személyek tudása és szakmai intelligenciája nélkülözhetetlen egy-egy szervezetre, vagy elektronikus információs rendszerre vonatkozó eljárásrend és feladatrendszer kialakítása és a szükséges összehangolási lépések kialakítása és fenntartása során.
    - A napjainkban azonosítható trendek, általános katonai követelmények követése érdekében elektronikus információvédelmi, elektronikus információbiztonsági, kibervédelmi területű (fejlesztésre, szervezésre vonatkozó) lépések történtek és történnek, ugyanakkor a meglévő szabályozók felülvizsgálata, pontosítása és összehangolása nem történt meg.

---

[74] PÁLL-OROSZ Piroska: Attribúció (betudás) a kibertérben; Nemzetbiztonsági Tanulmányok II. 2021; p. 81. ISBN 978-615-6128-04-01

[75] KOVÁCS László: Offenzív kiberműveletek 1: Az offenzív kiberműveletek természete; Hadmérnök, 2021/2. pp. 195-198.

- A katonai műveletek kibervédelmi támogatására irányuló szándék, cselekvésre vonatkozó törekvés több szinten azonosítható.
    - A kibervédelem (vagy egyéb kibertér-művelet/műveleti elem) katonai műveletek tervezésébe és a végrehajtásba történő integrálásának fontossága elismert, a komplex gondolkodás a gyakorlatban még nem valósult meg.
    - A katonai műveleti és doktrinális dokumentumok megfogalmazásai nem biztosítanak egységes értelmezési, szabályozási környezetet a végrehajtók számára.

Várható stratégiai szintű fejlemények

A NATO-tagállamok elkötelezték magukat 2022-ben egy új Stratégiai Koncepció kiadásában, ami védelempolitikai szinten kibervédelmi követelmények megjelenítését vetíti előre.

Az EU Kibervédelmi Szakpolitikai Program 2022-ben megújul, ami EU-szinten a katonai követelmények pontosításának érkezését jelzi.

Az EU Katonai Vízió és Stratégia a Kibertér, mint Műveleti Terület Alkalmazására dokumentum[76] 2021-es kiadása egyrészt felzárkózást jelent a NATO hasonló erőfeszítéseihez, másrészt előrevetíti a 2022-ben várható EU által vezetett műveletek és missziók kibervédelmi koncepciójának megújítását, benne együttműködési és információcsere követelményeinek meghatározását.

Az előbbiek mellett a NATO, EU és nemzeti folyamatok követése alapján kijelenthető, hogy további, a kibertérben történő működést szabályozó központi lépések, jogszabályi változások várhatók. E kérdések az ellenállóképesség vonalán a létfontosságú infrastruktúra üzemeltetőket (benne a honvédelmi érdekből kijelölt létfontosságú infrastruktúra érintettséget) is érinteni fogja, ahol megoldásokat kell találni az együttműködés, az információcsere kérdéseire. Az infrastruktúraüzemeltetők felé nemzeti szinten olyan támogatásokat kell kialakítani, ahol a fő kérdés szolgáltatás orientáltan a „hogyan lehet a legjobban segíteni" típusú felvetések kezelése az esetenként szakmai véleményként elhangzó felügyelet, irányítás átvétele és egyéb hasonlóan aggreszív és kevésbé hatékony eszközök bevetése helyett.

Honvédelmi területen még az idei év kihívása lesz, hogy a Hvt. említett változásai mellett a törvény új kiadása (vagy jelentős mértékű átalakítása) várható az Alaptörvény változásai alapján.

A védelemről és biztonságról szóló törvény megjelenése további jelentős mértékű változásokat fog indítani 2023-tól.

[76] European Union Military Vision and Strategy on Cyberspace as a Domain of Operations (2021).

Az előbbiekben vázolt jogszabályi változások mellett az új Nemzeti Biztonsági Stratégia, illetve a 2021-es Nemzeti Katonai Stratégia végrehajtásával kapcsolatosan is jelenhetnek meg új feladatok.

A 2018-as Hálózatbiztonsági Stratégia 2022-es cselekvési horizontjának közeledése, illetve önmagában a 2013-as Nemzeti Kiberbiztonsági Stratégia megújításának szükségszerűsége is jelzi a szakmai cselekvési irányokra, követelményekre vonatkozó pontosítások megjelenésének valószínűségét.
Technikai területen a nemzetközi folyamatokat követve újabb képességeket kell kialakítani a preventív és reaktív védelem fejlesztése érdekében, mint

- ***a honvédelmi ágazati korai előrejelző rendszer*** működését megalapozó jogszabályi környezet, a működést biztosító alacsonyabb szintű szabályozók kialakítása és szükséges technikai és információs folyamatok, a működési rend biztosítása, a védelmi rendszerek „előtti", megelőzést biztosító védelmi vonal kiépítése;
- a védelmi megoldások megbízhatóságának növelése érdekében az EU-s követelményeknek megfelelően ***kibervédelmi terméktanúsításra vonatkozó honvédelmi feladatrendszer*** kialakítása és bekapcsolása a nemzeti tanúsítási rendbe.

Technikai területen kihívást fog jelenteni, hogy a „Nemzeti Mesterséges Intelligencia Stratégia 2020" dokumentum a honvédelem területén feladatokat jelöl ki, mint tömegadat-feldolgozás, információvá szintetizálás, információs műveletek, döntéselőkészítő és -támogató rendszerek automatizálása, modellezés és szimuláció, illetve katonai nemzetbiztonsági területen célként azonosítja a katonai felhasználású kibertér védelmének MI-alapú támogatását.[77]

A már korábban említett magyar részvételű PESCO-projektek mellett említésre érdemes a portugál vezetésű Kiberakadémia és Innovációs Központ-kezdeményezés, valamint az idén februárban megjelenő, észt vezetésű „Cyber Range Federation" projekt. A két kezdeményezés más megközelítésben, de az oktatás, képzés és gyakorlás lehetőségeit fogja továbbgondolni. Új gondolat, hogy a kiber-PESCO-projektek esetében lehetőséget kell biztosítani a függetlenül kialakított képességek együttműködésére, „cluster"-ek létrehozására. (Például mindkét magyar részvételű projekt igényel technikai és magasabb szintű képzési támogatást, ami ezen az úton talán könnyebben megvalósítható lesz.)[78]

A jogszabályok követelményeinek végrehajtása érdekében a katonai műveletek tervezési és irányítási folyamataiban a mindenkori képességállapotnak megfelelő szinten[79] meg kell jeleníteni a kibertér-műveleti kérdéseket:

- módosítani kell a meglévő általános művelettervezési folyamatokat, aktualizálni kell a doktrinális kérdéseket és

---

[77] Nemzeti Mesterséges Intelligencia Stratégia 2020, 4.2.4 Államigazgatás – „Adatvezérelt szolgáltató állam" fejezet.

[78] Cyber PESCO Projects Conference (2022. 05. 23.) https://www.defesa.gov.pt/pt/pdefesa/CAIH/en/eucaih (Letöltés ideje: 2022. 06. 10.)

[79] Ez azt jelenti, hogy a honvédelmi struktúra aktuális állapota (hatáskörök, felelősségek) és az alkalmazott technológiák szerint kell a szükséges folyamatokat kialakítani és a jövőbeli fejlesztési elgondolásokat megfogalmazni.

- a műveleti tervekben folyamatosan át kell vezetni a szükséges változásokat.

A most ismert szabályozói környezetből levezetett új feladatok mellett a szövetségi követelmények továbbfejlődése, a honvédelmi képességek fejlesztése az eddigi tapasztalatok alapján számtalan esetben fog új szabályozási kihívásokat támasztani, illetve ugyanezen kérdések sürgetik a korábbi szabályok, eljárások felülvizsgálatát, pontosítását.

A különböző nemzetközi szereplők, programok összekapcsolásától szinergikus hatások várhatók. A mesterséges intelligencia, gépi tanulás, automatizáció, „Big Data", kvantumtechnológia és egyéb kihívások egyértelműen összetett, állami szintű válaszokat kívánnak az EU-tagállamoktól, talán legfontosabbként említve a képzett szakemberek meglétét és a kettős technológiák felhasználását.[80]

A nemzetközi és nemzeti követelmények továbbfejlődése, az új biztonsági, honvédelmi és katonai nemzetbiztonsági igények megjelenése, az új elektronikus szolgáltatások védelmi igényeinek komplex biztosítása technikai szinten folyamatos nyomás alatt fogja tartani a szakmai irányító, tervező és felügyelő honvédelmi szereplőket, és az új szolgáltatások kialakításában (leszállításában, tesztelésében, beüzemelésében, engedélyeztetésében) érintett szervezeteket, partnereket és cégeket.

Összefoglalás, következtetések

Az egész világon tapasztalható digitalizáció hazánkban is rengeteg eljárási, technikai változást hozott ebben az évezredben.

A honvédelmi területű működési keretrendszer ebben az időszakban nagyságrendekkel bonyolultabbá vált. Ráadásul az is kockázat nélkül jósolható, hogy a digitális fejlődés nem tekinthető lezártnak… Ez a gondolat kifejezetten védelmi szempontból azt világítja meg, hogy a bonyolultabbá váló szolgáltatások sérülékenysége, a sérülékenységek kihasználási módja, illetve az arra irányuló ellenséges szándék megléte kapcsán ***egyre szofisztikáltabb jelenségek várhatók a nemzetközi és nemzeti játéktérben egyaránt.***

A honvédelmi célú elektronikus információs rendszerek szükséges mértékű védelme érdekében az elektronikus információbiztonsági/információvédelmi, az üzemeltetői és a kibervédelmi szakterület szoros együttműködési kényszere mellett ***az egyéb szakmai területek felé irányuló fokozottabb szakterületi támogatási igény is jól tapintható*** (a teljesség igénye nélkül említve pl. a védelemigazgatási, jogi, védelempolitikai, műveletтervezési, haderőfejlesztési és humán területeket).

Honvédelmi területen jól érzékelhető, hogy ***az elektronikus információs rendszerek üzemeltetésére, használatára illetve biztonságára vonatkozó eljárások, folyamatok több szabályozói szinten és több területen fejtik ki hatásukat – időben is széttagoltan.*** Ennek a rendnek – normális esetben – előnye, hogy sikeres szabályozás

[80] EU cyber resilience challange (2022. 05. 25.); https://www.ucm.es/file/save-the-date-cyber-pesco-conference/?ver (Letöltés ideje: 2022. 06. 10.)

esetén az érintett szereplők (személyek vagy szervezetek) egyértelműen azonosíthatják a szolgáltatásokkal, rendszerekkel kapcsolatos lehetőségeket, folyamatokat, feladatokat, illetve a szükséges együttműködési lépéseket.[81] Az előnyök ellen hat az a hátrány, ami az összehangolással, változáskövetéssel kapcsolatos szakmai vezetői felelősséget és végrehajtói terhelést jelenti.

Ebben a helyzetben „kristálygömbje" válogatja, hogy milyen vezetői, szakmapolitikai és szakmai lépések tekintendők egyedüli, kizárólagosan jó megoldásnak, gyógyírnak a honvédelmi célú elektronikus információs rendszerek biztonsága növelése érdekében. A katonai vezetési és irányítási folyamatok összetettsége, a szakterületek eltérő témájú legégetőbb problémái vagy éppen legjobban kommunikálható lépései, illetve a folyamatos időprés hatása alatt jó megoldás aprólékos munkával, nehezen – és nagy szerencsével – alakítható ki.

Gyakori megoldás ilyenkor egy új szervezet vagy szervezeti elem megalakítása, átalakítása vagy egy új szakterületi központi követelmény (szabályozó) megjelenése a kívánt szakmai minőségi ugrás biztosítása érdekében.[82]

Jelen helyzetben ezek a megoldások nem tekinthetők garantálhatóan eredményesnek. Hasonlattal élve ez azt jelenti, hogy eltérő méretű és formájú boltívek hiába épülnek egy helyszínen, belőlük csak meghatározhatatlan, torz építmény születhet, kupola viszont nem. Emiatt a már megkezdett technikai lépések, kialakuló modern üzemeltetési és biztonsági folyamatok folytatása mellett szakmai szempontból egy előkészítő, „nulladik" lépés megtétele logikusabb megoldásnak tűnik.

A cselekvési alternatívák feltárását, a helyes fontossági sorrend kialakítását meg kell alapozni egy olyan felülvizsgálattal, ahol az előnyök, hátrányok azonosítása mellett megtörténik a folyamatok (és szervezetek, feladatok) közötti függőségek pontos feltárása, amelyet egy legalább stratégiai szintű kockázatelemzéssel és értékeléssel kell megerősíteni. Az így kialakult reális helyzetkép alapot biztosít felelős vezetői döntések megalapozásához, a szükséges szakmai cselekvési lépések megfogalmazásához. Megtörténhet az üzemeltetési, biztonsági és kibervédelmi folyamatok megerősítése (pl. folyamatok pontosítása, képzési és gyakorlási célok kitűzése), a katonai vezetési és irányítási rendszerben szükséges módosítások megtétele, illetve a kibervédelmi (tágabban: kibertér-műveleti) „gondolkodás" stratégiai, hadműveleti és harcászati szintű beágyazása a kor követelményeinek megfelelően.

A fenti lépések megtétele ellen számtalan, a napi életben folyamatosan – gyakran figyelmeztető jelek nélkül – jelentkező hatás (igény, követelmény) léphet fel. A nyilvánosság is jól követheti a haderőfejlesztés fontosabb történéseit, és a korábban nem tapasztalható ütemben történő légi, légvédelmi, szárazföldi haditechnikai rendszerek, eszközök megjelenését és alkalmazásba vételi igényét, amelyeket

---

[81] Pld. egy felhasználó a rendelkezésére álló információs környezetben mire jogosult, mit tehet, vagy nem tehet, hogyan kérhet segítséget; egy parancsnoknak milyen szervezeti elemeket, szabályozókat kell kialakítania.

[82] Mindkét megoldásra hozhatók példák, de kiemelendő, hogy megfelelő szervezeti, anyagi támogatás és a szükséges tudás megléte nélkül sem egy új szervezet, sem egy új központi szabályozó nem hozhat tartós szakmai fejlődést.

számtalan, „láthatatlan” üzembehelyezési, fenntartási és képzési feladathalmaz kísér, nehezít. Ezek a tényezők a rendelkezésre álló erőforrásokat gyakran a napi legsürgősebb ügyek megoldására rendelik, a jelenleg is sokszínű elektronikus adatkezelés palettájának további színesítésével – és az összkép még bonyolultabbá tételével.

Az előbbiek megalapozzák a következtetést, hogy a jelenlegi helyzetben a honvédelmi célú elektronikus információs rendszerek biztonságának növelése rengeteg új folyamat megjelenését és fenntartását igényli, ami a rengeteg kérdőjel mellett az ismeretlen függőségi kapcsolatok, a támogatói lánc-kockázatok, a tudásban vagy telepítésben (beüzemelésben) lévő esetleges hiányosságok felkiáltójeleit is magukkal hordozzák.

Ezek mellett ***kiemelt fontosságúnak kell tekinteni a meglévő működési keretrendszer felülvizsgálatát, pontosítását,*** és a stratégiai szintű kockázatok azonosítására, értékelésére alapozott kockázatkezelési lépések megtételét.

Egyszerűen kifejezve kijelenthető, hogy ***megbízható, szilárd alapok nélkül kockázatos az építkezés!***

Köszönet a vizsgálat szakterületein dolgozó, aktívan szolgáló kollégáknak, oktatóknak, civil szakterületi szakértőknek és nyugdíjas kollégáknak, akik gondolataikkal segítettek vagy korábbi erőfeszítéseikkel hozzájárultak a biztonsági kérdések megoldásához!

Felhasznált irodalom:

- 10/2012. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről
- 10/2015. (III. 26.) HM utasítás a Magyar Honvédség egyes szervezetei feladatrendszerének módosításával és vezetési rendszerét érintő átalakításokkal kapcsolatos egyes feladatokról, 3. § 1-2. p. (hatályon kívül).
- 13/2016. (HK 7.) HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszerek biztonsági akkreditációs eljárásrendjéről
- 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
- 14/2021. (III. 19.) HM utasítás a honvédelmi szervezet 2021. évi kiemelt feladatainak, valamint a 2022–2023. évi fő célkitűzéseinek meghatározásáról
- 15/2017. (IV. 28.) HM utasítás a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól

- 1500/2015. (VII. 23.) Korm. határozat a Magyar Honvédség kibervédelem szempontjából kiemelt jelentőségű komplex informatikai fejlesztéseihez kapcsolódó beszerzéseknek a védelem terén alapvető biztonsági érdeket érintő, kifejezetten katonai, rendvédelmi, rendészeti célokra szánt áruk beszerzésére, illetőleg szolgáltatások megrendelésére vonatkozó sajátos szabályokról szóló 228/2004. (VII. 30.) Korm. rendelet
- 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről (hatályon kívül).
- 175/2022. (HK 4.) MH PK intézkedés a Magyar Honvédség Kibertér műveleti doktrína (1. kiadás) című szolgálati könyv kiadásáról
- 18/2016. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszerek Rendszer Biztonsági Követelményeire vonatkozó szabályokról
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
- 20/2013. (HK 12.) HVK HIICSF szakutasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszer-specifikus elektronikus biztonsági követelményeinek meghatározásáról
- 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 (Ibtv.)
- 22/2016. (II. 17.) 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 szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról
- 259/2021. (V. 20.) Korm. rendelet a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról
- 3/2012. (01. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról
- 3/2022. (I. 27.) HM utasítás a honvédelmi szervezet 2022. évi kiemelt feladatainak, valamint a 2023–2024. évi fő célkitűzéseinek meghatározásáról
- 30/2021. (VII. 23.) HM utasítás a „Létfontosságú Védőbástya 2021” nemzeti létfontosságú rendszerelemeket érintő válságkezelési gyakorlat honvédelmi ágazatot érintő feladatainak előkészítéséről és végrehajtásáról
- 32/2021. (VII. 23.) HM utasítás a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról
- 39/2014. (V. 30.) HM utasítás a Magyar Honvédség Informatikai Szabályzatának kiadásáról
- 42/2020 HM utasítás egyes NATO egységesítési jelzések elfogadásáról
- 5/2014. HVK HIICSF szakutasítás a honvédelmi tárca elektronikus adatkezelő rendszerek incidenskezelési eljárásrendről

- 58/2014. (IX. 10.) HM utasítás a Magyar Honvédség Informatikai Stratégiájának kiadásáról
- 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról
- 75/2013. (XII. 5.) HM utasítás a Magyar Honvédség Rejtjelszabályzat kiadásáról
- 81/2011. (VII. 29.) HM utasítás a honvédelmi tárca Kibernetikai Védelmi Koncepció kialakításához szükséges feladatok meghatározásáról
- 9/2012. HVK HIICSF szakutasítás a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről
- 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról
- A visegrádi országok katonai kibervezetői tanácskoztak Budapesten (2021. 11. 15.), https://honvedelem.hu/hirek/a-visegradi-orszagok-katonai-kibervezetoi-tanacskoztak-budapesten.html (Letöltés ideje: 2022. 06. 10.)
- Átadták a Magyar Honvédség Kiber Képzési Központját; https://honvedelem.hu/media/aktualis-videok/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat.html (Letöltés ideje: 2022. 06. 10.)
- Átfogó képet kaptak a kibertér védelméhez szükséges módszerekről és eszközökről; https://honvedelem.hu/hirek/hazai-hirek/atfogo-kepet-kaptak-a-kiberter-vedelmehez-szukseges-modszerekrol-es-eszkozokrol.html (Letöltés ideje: 2022. 06. 10.)
- Cyber defence exercise brings together military CERTs; https://eda.europa.eu/news-and-events/news/2021/02/19/cyber-defence-exercise-brings-together-military-certs (Letöltés ideje: 2022. 06. 10.)
- Cyber PESCO Projects Conference (2022. 05. 23.) https://www.defesa.gov.pt/pt/pdefesa/CAIH/en/eucaih (Letöltés ideje: 2022. 06. 10.)
- EDA MilCERT Interoperability Conference talks strategy https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy (Letöltés ideje: 2022. 06. 10.)
- EU cyber resilience challange (2022. 05. 25.); https://www.ucm.es/file/save-the-date-cyber-pesco-conference/?ver (Letöltés ideje: 2022. 06. 10.)
- European Union Military Vision and Strategy on Cyberspace as a Domain of Operations (2021).
- FARKAS Ádám: A kortárs technikai-fejlődés és innováció viszonya a honvédelmi szabályozással; MTA Law Working Papers, 2021/4. ISSN 2064-4515
- FARKAS Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán; Military and Intelligence Cyber Security Research Paper 2021/1;
- Fókuszban a kiberbiztonság (2021. 09. 17), https://honvedelem.hu/hirek/fokuszban-a-kiberbiztonsag.html (Letöltés ideje: 2022. 06. 10.)

- GERŐFI Szilárd: A Magyar Honvédség vezetéstámogató rendszere alkalmazásának lehetőségei a XXI. századi kihívások tükrében; Hadtudomány, 2017/3-4. pp. 96-105.
- HM-MH Titokvédelmi és Ügyviteli Szabályzat – Ált/3. 1996.
- http://tavoktatas.mil.hu/tudatossag/rolunk/index.html; 2022. (Letöltés ideje: 2022. 06. 10.)
- Hungary signs new MoU on cyber defence cooperation; https://nicp.nato.int/hungary-signs-new-mou-on-cyber-defence-cooperation/index.html (Letöltés ideje: 2022. 06. 10.)
- KASSAI Károly: A honvédelmi célú elektronikus információs rendszerek fejlesztéséhez szükséges továbblépés megalapozásához szükséges vizsgálat – egy zöld könyv kialakításának támogatása; Military and Intelligence Cybersecurity Research Paper, 2022/5.
- KASSAI Károly: A honvédelmi tárca biztonságpolitikájában meghatározott követelmények, feladatok és azok fontosabb hatásai; Hadmérnök, 2009/4. pp. 183-190.
- KASSAI Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban; Hadmérnök, 2015/3.
- KASSAI Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban; Hadmérnök, 2015/3.
- KASSAI Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban; Hadmérnök 2015/3.
- KELEMEN Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése; Military and Intelligence Cyber Security Research Paper, 2022/1.
- KNAPP Gábor: Az elektronikus információbiztonság- tudatosítás feladatrendszerének honvédelmi ágazati szempontú vizsgálata és kihívásai; Szakmai Szemle XVIII. évfolyam 3. szám.
- KOVÁCS László: Offenzív kiberműveletek 1: Az offenzív kiberműveletek természete; Hadmérnök, 2021/2.
- MAGYAR Sándor: Katonai kibertér 2021. Konferencia beszámoló; Szakmai Szemle 2021/4.
- Magyarország élen jár az európai katonai kibervédelemben; https://honvedelem.hu/hirek/magyarorszag-elen-jar-az-europai-katonai-kibervedelemben.html (Letöltés ideje: 2022. 06. 10.)
- Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat
- Magyarország Nemzeti Katonai Stratégiájának elfogadásáról szóló 1656/2012. (XII. 20.) Korm. határozat
- Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat
- MEZŐ András: A Magyar Honvédség doktrínafejlesztése – 2. rész; Hadtudomány, 2018/1. pp. 48-57.

- MOLNÁR Anna – SZABOLCS Laura: Megerősített együttműködés, változó geometria. PESCO; Hadtudomány 2020/4.
- NATO Walesi Nyilatkozat, 2014. szeptember 05. (72. pont). NATO Varsói Nyilatkozat 2016. július 09. 71-72. pont
- Nemzetközi Katonai Információbiztonsági Konferencia (2022. 05. 03.); https://honvedelem.hu/hirek/nemzetkozi-katonai-informaciobiztonsagi-konferencia.html (Letöltés ideje: 2022. 06. 10.)
- PÁLL-OROSZ Piroska: Attribúció (betudás) a kibertérben; Nemzetbiztonsági Tanulmányok II. ISBN 978-615-6128-04-01, 2021.
- Sikeresen lezajlott a magyar kiberbiztonsági gyakorlat (HunEx2019); https://nki.gov.hu/intezet/kozlemenyek/sikeresen-lezajlott-a-magyar-kiberbiztonsagi-gyakorlat (Letöltés ideje: 2022. 06. 10.)
- SPITZER Jenő: A francia kibervédelmi és kiberbiztonsági rendszer egyes stratégiai aspektusai; Military and Intelligence Cyber Security Research Paper 2021/3.
- SZENTGÁLI Gergely: A magyar kibervédelem anatómiai képe; Felderítő Szemle, 2013. december, pp. 74-89. HU ISSN 1588-242X
- VASVÁRI Géza: a katonai szervezetek elektronikus információvédelmi képességeinek fejlesztésével kapcsolatos feladatok, Hadtudományi Szemle, 2018/5.
- VIKMAN László: A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására; Military and Intelligence Cyber Security Research Paper 2021/2.

DR. ALBERT ÁGOTA – ÜVEGES ANDRÁS JÓZSEF

AZ „IoT”-ESZKÖZÖK BIZTONSÁGA A SZEMÉLYES ADATOK TÜKRÉBEN

Problémafelvetés

Az IoT[1]-eszközök felhasználása a digitalizációs folyamatok felgyorsulása miatt egyre gyorsabban terjed. Mivel a honvédelmi ágazatban is egyre több IoT-eszköz kerül alkalmazásra, így most már egyre több esetben kell vizsgálni ezen eszközök kiberbiztonsági, információbiztonsági és nemzetbiztonsági kockázatait. Fontos kiemelni azt is, hogy az IoT-eszközök nem csak a honvédelmi szektorban alkalmazott informatikai rendszerek elemeiként jelenhetnek meg, hanem a hivatásos katonák, köztisztviselők és kormánytisztviselők, beszállítók munkatársainak személyes használati tárgyaként is. Így szükségszerű ezt a jelenséget is vizsgálni, mivel a napi tevékenység végzése közben számos, eddig nem használt IoT-eszköz jut be honvédelmi érdekeltségű területekre.

Hipotézis

Az IoT-eszközök jelentős nemzetbiztonsági kockázatot okozhatnak akkor, ha nem vizsgáljuk megjelenésük és gyors terjedésük okozta kockázati tényezőket. Jelenleg nincs rendszerezve, megbecsülve, valamint osztályozva, hogy milyen csatornákon milyen kockázati tényezőt jelent az érzékeny adataink kiszivárgása ezen eszközökön keresztül. Elgondolásunk szerint az IoT-eszközök gyors és kontroláltalan terjedése miatt a honvédelmi ágazaton belül van egy küszöbszint, ahol a személyes adatok kiszivárgásának a lehetősége eléri azt a pontot, hogy az már nemzetbiztonsági kockázatot jelenthet a szervezetre nézve. Ezen kívül elgondolásunk szerint számos informatikai, hobbi- és általános otthoni felhasználásra szánt eszköz válik úgy IoT-eszközzé, hogy arról annak felhasználója nem tud, és azt saját hibáján kívül beszállítja honvédelmi célú objektumba.

Bevezetés

Globális tekintetben az IoT-eszközök terjedése exponenciális jelleggel nő. A Findstack[2] adatai szerint 2021-ben[3] már 35.82 milliárd IoT-eszköz működik világszerte, 2025-re várhatóan már 38.6 milliárd ilyen eszköz lehet hálózatba kapcsolva,[4] 2030-ra pedig ez a szám eléri majd az 50 milliárdot. Jelen tanulmányban kísérletet tesztünk a kockázatok és ezek hatásainak rendszerezésére, valamint átfogó képet kívánunk nyújtani arról, hogy milyen jogszabályok vonatkoznak ezekre az

[1] Internet of Things – dolgok internete

[2] A Findstack segítségével vállalkozásunk számára kereshetünk szoftver környezetet és modulokat az on-line szolgáltatásokhoz.

[3] 2018-ban megközelítőleg 22 milliárd eszköz volt hálózatba kötve.

[4] JACK Steward: The Ultimate List of Internet of Things Statistics for 2021. Findstack. 2021. https://findstack.com/internet-of-things-statistics/ (Letöltés ideje: 2022. 02. 21.)

eszközökre. Írásunkban törekszünk arra is, hogy azonosítsuk az összes csatornát ahhoz, hogy felmérhessük, a honvédelmi ágazatban mekkora kockázatot jelentenek a szervezetszerűen rendszeresített IoT-eszközök, vagy az eddig nem ismert módon beszállított IoT-termékek.

IoT-eszközök definíciója

A tanulmány könnyű és dinamikus értelmezéséhez lényeges azt röviden áttekinteni, hogy ma hogyan értelmezhető az IoT fogalma. A kifejezést ismereteink szerint Kevin Ashton használta először: *„Lehet, hogy tévedek, de biztos vagyok benne, hogy a "Tárgyak internete" kifejezés egy 1999-ben a Procter&Gamble (P&G) vállalatnál tartott előadásom címeként indult. Az RFID új ötletének összekapcsolása a P&G ellátási láncában az internet akkoriban felkapott témájával több volt, mint egy jó módja annak, hogy felkeltsem a vezetők figyelmét."*[5]

Az „IoT", mint fogalom 2010-re már világszerte elterjedt, amelynek köszönhetően ma már számtalan meghatározásával találkozhatunk attól függően, ki milyen szempontok alapján próbálja definiálni a fogalmat (eszközöket).

Az ENISA[6] meghatározása szerint a tárgyak internete *„az egymással összekapcsolt érzékelők és működtetők kiberfizikai ökoszisztémája, amely intelligens döntéshozatalt tesz lehetővé".*[7] Az ügynökség a tárgyak internetének középpontjába az információt helyezi.

A 29. cikk szerinti Adatvédelmi Munkacsoport 2014-ben adta ki a tárgyak internetével foglalkozó véleményét[8]. A dokumentum megfogalmazása szerint: *„A tárgyak internete (Internet of Things) olyan infrastruktúrára utal, amelyben a mindennapi eszközökbe (önálló „dolgokba" vagy egyéb tárgyakhoz vagy személyekhez kapcsolodó dolgokba) beépített érzékelők milliárdjait arra tervezik, hogy adatokat rögzítsenek, kezeljenek, tároljanak és továbbítsanak, és – mivel egyedi azonosítóval rendelkeznek – a hálózati szolgáltatások segítségével együttműködjenek más eszközökkel vagy rendszerekkel."*[9].

Az Amerikai Egyesült Államok Kalifornia állam 2020. január elsejétől alkalmazandó „IoT-törvénye" a kapcsolódó eszközök oldaláról határozza meg az IoT fogalmát: *„minden olyan eszköz vagy más fizikai tárgy, amely közvetlenül vagy közvetve képes csatlakozni az internethez, és amelyhez internetprotokoll-cím vagy*

---

5 ASHTON, Kevin: That 'Internet of Things' Thing In the real world, things matter more than ideas, 2009. június 22, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf (Letöltés ideje: 2021. 06. 09.)

6 Európai Uniós kiberbiztonsági Ügynökség – The European Union Agency for Cybersecurity; https://www.enisa.europa.eu/about-enisa/ (Letöltés ideje: 2021. 06. 09.)

7 ENISA: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 2017. november, 12. o.

8 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16. (továbbiakban: WP223)

9 Uo. p. 4.

Bluetooth-cím tartozik."[10], valamint az Amerikai Egyesült Államok 2020. decemberi IoT-törvénye[11] szerint *„A tárgyak internete olyan eszközök, amelyek - (A) legalább egy, a fizikai világgal közvetlen kölcsönhatásba lépő átalakítóval (érzékelő vagy működtető) rendelkeznek, legalább egy hálózati interfészük van, és nem hagyományos információtechnológiai eszközök, mint például okostelefonok és laptopok, amelyek esetében a kiberbiztonsági jellemzők azonosítása és megvalósítása már jól ismert; és és (B) képesek önállóan működni, és nem csak akkor képesek működni, ha egy másik eszköz, például egy processzor alkotóelemeként működnek."*

A magyar jogalkotásban a nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól szóló 7/2015. (XI. 13.) NMHH rendelet 2020. október 20 óta hatályos értelmező rendelkezései alapján az *„99b. IoT: általában olyan, használati tárgyakba beépített eszközök interneten keresztüli összekapcsolása, amely eszközök lehetővé teszik ezen használati tárgyak közötti adatcserét; 99c. IoT rendszer: IoT-t megvalósító rádiótávközlő rendszer, különösen az EC-GSM-IoT, LTE-MTC, LTE-eMTC, NR-IoT és NB-IoT rendszer*"[12].

A magyar jogalkotásban található definíció az IoT és az IoT-rendszerek fogalmát meglehetősen szűken értelmezi, „általában" használati tárgyakba épített eszközökre, illetve az IoT-t megvalósító távközlő rendszerre korlátozza (leginkább a 2014-es 29. cikk szerinti Adatvédelmi Munkacsoport meghatározására emlékeztetve), miközben nemzetközi szinten már IoT-ökoszisztémákban (például IPAR 4.0) gondolkodnak a szakemberek.

Ezen definíciók mellett érdemes megnézni a Wikipédia szócikkét is, hiszen az ebben szereplő meghatározás az, amellyel a legtöbb interneten böngésző felhasználó legelőször találkozik. A szócikk szerint *„dolgok internetje (angolul: Internet of Things, rövidítve: IoT) lényegében olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internet alapú hálózaton egy másik eszközzel kommunikálni. A fogalom más szavakkal hálózatba kötött „intelligens" eszközöket takar, amelyek a beépített érzékelők és szenzoroknak köszönhetően képesek adatokat gyűjteni."*

A gartner.com még ennél is egyszerűbb megfogalmazásra törekszik, miszerint a *„tárgyak internete (Internet of Things, IoT) olyan fizikai tárgyak hálózata, amelyek beágyazott technológiát tartalmaznak a kommunikáció és a belső állapotukkal vagy a külső környezettel való érzékelés vagy kölcsönhatás érdekében."*[13]

---

[10] Civil Code – CIV. Division 3. Obligations [1427 – 3273.16]. Part 4. Obligations Arising From Particular Transactions [1738 – 3273.16]. Title 1.81.26 – Security of Connected Devices 1798.91.05; https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.26.&part=4.&chapter=&article=, (Letöltés ideje: 2022. 02. 20.)

[11] Internet of Things Cybersecurity Improvement Act of 2020 Sec. 2. (4), 2020. december 4. https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf (Letöltés ideje: 2020. 02. 20.)

[12] A nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól szóló 7/2015. (XI. 13.) NMHH rendelet 2.§ (1) bekezdés 99.b és 99.c. pontok

[13] https://www.gartner.com/en/information-technology/glossary/internet-of-things (Letöltés ideje: 2022. 02. 20.)

Napjainkban már a „civil” térhódítás mellett az IoT honvédelmi ágazati megjelenését is vizsgálni kell, különös tekintettel arra, hogy ezzel a technológiával számos hadiipari vállalat is foglalkozik. Ezek a cégek egyre komolyabb erőforrásokat fordítanak arra, hogy az IoT-eszközökre épülő megoldások segítségével fejlesszék a gépi tanulást, illetve automatizálják a katonai döntéshozatali rendszereket. Az IoT katonai alkalmazásának lehetőségének vonatkozásában számos mű készült, ezek alapvetően úgy értékelik, hogy az IoT-eszközök megjelenése elkerülhetetlen a haderőben.

Kollár Csaba 2017-ben művében röviden összefoglalta azt, hogy *„a hálózatos katona az utópisztikus távoli jövőből kézzelfogható távolságba, több területen pedig már a jelen valóságába került”,*[14] 2021-ben pedig ez már nem utópia, hanem maga a realitás. A tanulmány alapvetően jól összefoglalja a fejlesztési irányokat, és foglalkozik az információbiztonság kérdéskörével is.

Ugyanezt az elgondolást támasztja alá az is, hogy az IoT-eszközök közigazgatási alkalmazásával kapcsolatban már 2015-ben is születtek koncepciók, Haig Zsolt írásában pedig megjelenik ez az elgondolás is, miszerint: *„A közigazgatási rendszerekben az ügyfélszolgálatok hatékonysága javítható, illetve az online ügyfélszolgálatok terén nyújthatnak plusz lehetőségeket az IoT-megoldások”.*[15] A publikáció előremutatóan meghatároz három olyan katonai területet, ahol az IoT-eszközök alkalmazhatóak:

- logisztika – az összfegyvernemi műveletek logisztikai támogatásának vezetési és irányítási lehetőségei, valós idejű készlet- és szállítókapacitás kezelése,[16] GPS-követés, gépjárműmotor-élettartam-menedzsment, üzemanyag-felhasználás mérése,[17] a gépjárművezetők tevékenységének monitorozása szenzorokkal későbbi kiértékeléshez.[18] Egyes esetekben a rendszer bonyolultsága és komplexitása miatt ezeket két külön kérdésként kezelik, az egyikben a gépjárműmozgással kapcsolatos IoT-eszközöket csoportosítják, a másik esetben pedig a klasszikus értelemben vett katonai logisztikát különítik el (hadfelszerelés-menedzsment);
- helyzetismeret;
- egészségügyi ellátás.[19]

Amellett, hogy a fogalmat tisztázzuk, a kockázatok beazonosítása és kezelése érdekében azt is fel kell tárni, hogy az IoT-eszközök vonatkozásában hol jelenik meg közvetlenül a személyes adatok védelmének kérdésköre.

---

[14] KOLLÁR Csaba: Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai, Hadmérnök, 2017/4. pp. 146-158.

[15] HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest, 2018. p. 98.

[16] Gyakorlatilag a polgári életből vett flottakezelés katonai megfelelője.

[17] Az Amerikai Egyesült Államok Védelmi Minisztériuma szerint 25% csökkenthető a felhasználás IoT alkalmazása során.

[18] SHAU, Manisha: 7 Applications of IoT in Defence and Military. AnalyticStep, 2021 https://www.analyticssteps.com/blogs/7-applications-iot-defence-and-military (Letöltés ideje: 2022. 02. 20.)

[19] HAIG (2018) i. m. p. 121.

IoT a honvédelmi ágazatban

A tanulmányban alapvetően és döntően nem foglalkozunk részletesen azokkal az IoT-eszközökkel, amelyek a haderőbe a klasszikus értelemben véve rendszeresítésre kerülnek, azonban mindenképpen szeretnénk egy rövid áttekintés nyújtani e témában is, mivel fontos az, hogy az olvasó lássa, szervezetszerűen is bekerültek IoT (DIoT[20])-eszközök a honvédelmi ágazatba.

A megfogalmazást tekintve a nyílt források IoMT-[21] vagy IoBT[22]-eszközökként hivatkoznak a rendszeresített eszközökre. Tartalmilag az IoBT olyan eszközrendszereket foglal magában, amelyek teljes spektrumú (pervazív) érzékelést és kommunikációt biztosítanak a felhasználók részére. Az eszközrendszerek működése során nagy mennyiségű adat keletkezik, köszönhetően a nagyszámú szenzoroknak,[23] és az IoT területén ez okozza jelenleg a legnagyobb kihívást, mivel a katonák által viselt, valamint a harctérre előre telepített stacioner szenzorhálózatok együttesen nehezen kezelhető méretű adatmennyiséget termelnek.

Az IoT-eszközök a honvédelmi ágazatban jellemzően harcászati körülmények között jelennek meg, például olyan kiegészítőként, amit a katona önmagán visel, mint például biometrikus szenzor, biometrikus ellenség/barát-azonosító, vagy olyan eszköz, ami segíti a kezelőt hozzáférni egy adott fegyverrendszerhez. Ezek az eszközök nagy mennyiségű személyes adatot (nagyrészben az adatok különleges kategóriájába tartozó személyes adatot) kezelnek, mivel itt rögzítésre kerül a viselő személy arcformája, írisze, szívritmusa, arcának gesztusai és mintája is.

Kockázatelemzés

Általános kockázatok

Az IoT-ökoszisztéma általános problémáit az ENISA 2017-ben számba vette[24], a biztonsági szakembereknek, a gyártóknak–fejlesztőknek, és maguknak az érintetteknek szánt figyelmeztetésük 2022-ben is kiindulási pont, függetlenül attól, mi célt szolgál az adott rendszer, ezért jelen tanulmányunkban mi is ezt vesszük figyelembe:

– a támadási felület széles spektrumú, az IoT-rendszereket érintő fenyegetések és kockázatok komplexek, a technológia gyors fejlődése miatt változnak és folyamatosan fejlődnek, illetve ezen eszközök és rendszereknek gyakran jelentős hatást gyakorolnak a felhasználók (érintettek) egészségére, biztonságára és magánéletére is. Az IoT-rendszerekben az adatgyűjtés és az adatok kezelésének módja a felhasználók és egyéb érintettek számára gyakran nem egyértelmű, mivel az IoT nagymértékben a különböző forrásokból származó

[20] Defense Internet of Things
[21] Internet of Military Things
[22] Internet of Battlefield Things
[23] CASTIGLIONE Aniello – CHOO, Kim-Kwang Raymond – NAPPI, Michele – RICCIARDI, Stefano: Context Aware Ubiquitous Biometrics in Edge of Military Things; IEEE Cloud Computing, 2017/6. pp. 16-20. DOI: 10.1109/MCC.2018.1081072
[24] Az ENISA: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures; November 2017 alapján

nagy mennyiségű adat gyűjtésén, cseréjén és feldolgozásán alapul, amelyek között nagy mennyiségben található „érzékeny”[25] adat is;

- Egy-egy rendszerbe integrált különböző korú és gyártmányú eszközök műszaki tartalom alapján jelentősen különbözhetnek[26], ez pedig megnehezítheti, vagy akár meg is gátolhatja az elvárt szintű kommunikációt, valamint komoly biztonsági réseket is okozhatnak;
- Az IoT-eszközök és rendszerek biztonságának jelentős kockázati tényezője az is, hogy alacsony árszínvonalon tömeggyártásban is készülhetnek, és a költségtakarékosság miatt gyenge biztonsági megoldásokat tartalmazhatnak. Ezen „olcsó” eszközök rendszerbe integrálásukkal olyan komplex ökoszisztéma részévé válhatnak, amely jelentős mennyiségű adatot kezel, és amellyel szemben magas szintű bizalmassági, sértetlenségi és rendelkezésre állási követelmények vannak (CIA-elv[27]);
- A biztonsági követelményeket az IoT-rendszerek teljes életciklusában teljesíteni kell az eszközök/rendszerek tervezésétől a gyártáson, működésbe állításon, használaton és szervizelésen át egészen az ökoszisztémából kivonásig és a leselejtezésig (megsemmisítésig);
- A hagyományos biztonsági megoldások az IoT-ökoszisztémában a technikai korlátok miatt nem mindig alkalmazhatóak, mivel az eszközök többsége korlátozott képességekkel rendelkezik a memória, az energia és az adatfeldolgozás terén, emiatt a fejlett biztonsági ellenőrzések nem mindig alkalmazhatók kellő hatékonysággal;[28]
- Az IoT világa napról napra bővülő, változatos, széleskörű és bonyolult rendszer, amely nemcsak az eszközöket foglalja magában, hanem a kommunikációt, az interfészeket és magukat az embereket[29] is. A rendszer elemei akár egymástól függetlenül is cserélődhetnek, illetve üzemképtelenné válásuk esetén gyakran nem lehet ugyanolyan műszaki jellemzővel bíró másik eszközzel cserélni az elemeket. Az elemek „összetanítása” nem egyszerű feladat, a rendszer működtetése mindenképpen felügyeletet igényel;
- A komplexitás kérdése minden szinten jelen van. Az IoT-rendszerek és szolgáltatások középpontjában a szoftver áll, amely biztosítja az elvárt funkciókat, például az IoT-eszközök firmware-je, az IoT kommunikációs protokollok és -rendszerek implementációi, az IoT-termékek operációs rendszerei, a különböző IoT-szolgáltatások interoperabilitását és összekapcsolhatóságát támogató alkalmazás programozási interfészek, az IoT-interoperabilitást fokozó architektúrák, például a gyártói felhasználási leírás, az IoT-eszköz-illesztőprogramok, a háttértárt biztosító IoT-felhő és virtualizációs szoftverek, valamint egyéb különböző IoT szolgáltatási funkciókat megvalósító szoftverek. Egyre gyakoribb a mesterséges intelligenciát alkalmazó eljárások integrálása is az IoT-eszközökbe;
- A szabványok és szabályozások nem egységesek, az új szabályozók létrehozása lassú folyamat, és számtalan nehézségekbe ütközhet, miközben folyamatosan

[25] Különleges és bűnügyi adat
[26] Szabványok, tanúsítványok stb
[27] Confidentiality, Integrity, Availability
[28] Energiatakarékos üzemmódban korlátozott önvédelmi funkciók.
[29] Gyártók, alkalmazásfejlesztők, felhasználók, egyéb érintettek stb.

jelennek meg az új és még újabb technológiák, a rendszerek üzemeltetőinek pedig – adott esetben – integrálniuk kell ezeket a saját ökoszisztémájukba még akkor is, ha arra valójában nincs szükségük;

– Az IoT-eszközök nagyon gyorsan igen széles spektrumon elterjedtek, a magánhasználattól a kereskedelmi és ipari alkalmazások mellett a létfontosságú infrastruktúrák és az intelligens infrastruktúrák terén is. Ez a probléma különösen jelen van olyan területeken, mint például a vasúti közlekedés, amely olyan nagy infrastruktúraigényű ágazat, amelyben az üzembiztonság egy pillanatra sem elhanyagolható szempont, illetve területileg szétszórt, különböző korú elemeket tartalmaz, amelyeket számtalan szereplő működtet(het), miközben a jegyárakban az új fejlesztések csak erősen korlátozott mértékben érvényesíthetőek;

– A biztonsági szempontok fokozottan kell, hogy érvényesüljenek az IoT-ökoszisztémában, mivel a működtetők (kapcsolók) a fizikai világra hatnak. A fenyegetések számtalan emberéletet veszélyeztetnek (pld. ivóvízrendszer manipulálása, kőolajfinomító elleni szabotázsakció, vasúti szolgáltató ellen végrehajtott kibertámadások stb.). A biztonsági integráció nehézkes az esetlegesen egymásnak ellentmondó szempontok és követelmények miatt, a biztonsági szakemberek számára komoly kihívást jelenthet a különböző hitelesítési megoldásokon alapuló IoT-eszközök és rendszerek integrálása, és ezen rendszerek interoperábilissá tétele;

– Az IoT-eszközök számos ágazatban jelentős költségmegtakarítási lehetőségeket jelentenek az olyan funkcióik kihasználásával, mint például az adatáramlás, a fejlett felügyelet és az integráció. Azonban azt sem szabad figyelmen kívül hagyni, hogy a versenyképes árakra törekedő gyártók és alkalmazásfejlesztők gyakran a funkcionalitást és használhatóságot előtérbe helyezve a biztonsági funkciókon spórolnak, ezért nem garantált, hogy ezen eszközök (rendszerek) az elvárt szinten védettek a kibertámadások ellen. A helyzetet súlyosbítja, hogy az IoT-termékek piacra kerülése során, a gyártókon, fejlesztőkön hatalmas nyomás van a kiélezett verseny miatt, ez pedig jelentősen korlátozhatja azt az időt, amely a biztonsággal és a beépített adatvédelemmel kapcsolatos fejlesztésekre fordítható;

– Az IoT-eszközök és rendszerek esetében kiemelten fontosak a biztonsági frissítések, azonban problémát okozhat az, hogy számtalan esetben nem lehet alkalmazni a hagyományos frissítési eljárásokat, különösen az Over-The-Air[30] frissítések esetében;

– Az összetett rendszerek összetett felelősségi rendszereket eredményezhetnek, különösen a harmadik féltől származó elemek esetében. A nem tisztázott felelősségi viszonyok konfliktusokhoz vezethetnek, és már egy kisebb adatvédelmi incidens következményeinek csökkentése is komoly megpróbáltatásokat okozhat a szereplőknek. A személyes adatok kezelése tekintetében a GDPR és a bűnügyi adatvédelmi irányelv egyértelműsíti a felelősségi viszonyokat az adatkezelési konstrukciók területén (pld. adatfeldolgozás, közös adatkezelés), valamint az adatkezelők közötti adattovábbításnak is meg kell felelnie az elszámoltathatóság elvének, de ez még

[30] Over the Air – OTA, például a Volkswagen a szoftverorientált mobilitási szolgáltatásokkeretén belül a frissítéseket (ID.302: a legújabb „ID.Software2.3” szoftververziót) mobil adatátvitel útján 2021 júliusában juttatják el ügyfeleinek.

nem azt jelenti, hogy ezen jogszabályok hatálya alá tartozó IoT-rendszerek esetében maradéktalanul sikerül ezeket a szerepeket és felelősségi köröket megnyugtatóan tisztázni;

– Az adatvédelem és adatbiztonság területén az emberi hibák számának csökkentése érdekében az adatkezelőknek rá kell venniük a felhasználókat az együttműködésre (biztonsági tudatosság kialakítása), ennek hiányában az IoT-eszközök és rendszerek biztonsági kockázata jelentős mértékben növekszik;

– A gyorsan változó körülmények miatt egy adott védelmi módszer (pld. anonimizálási, titkosítási eljárás stb.) pár éve még megfelelő védelemnek bizonyulhatott, a mesterséges intelligencia fejlődésével és használatának elterjedésével azonban nem biztos, hogy ma is megfelelő. A biztonsági szakembereknek fel kell készülniük arra is, hogy pár év múlva még több, ma még biztonságosnak hitt módszertől kell búcsút venniük, és helyettük új megoldásokat kell rendszeresíteniük.

Figyelmet érdemlő példa az Otonomo[31] esete, amely az anonimizálásban rejlő buktatókra világít rá. Ez a cég mintegy 40 millió jármű pontos helymeghatározási adatait értékesíti szerte a világban, a helymeghatározási adatok egy részét pedig egy ingyenes próbaverzió keretében is elérhetővé teszi. Az adatok elvileg csak az autó nem körülírható azonosítójához[32] kapcsolódnak, de a Motherboard szerint[33] viszonylag könnyen kideríthető, hogy egy autó potenciálisan kihez tartozik, és követhető a mozgása is, például berlini és kaliforniai sofőrök GPS-koordinátái alapján meg lehet határozni azok valószínűsíthető lakcímét és személyazonosságát is. A cég által összegyűjtött adatok különböző helyekre, így biztosító társaságokhoz meg reklámcégekhez vándorolhatnak, de akár nemzetbiztonsági vagy hírszerzési célokra is felhasználhatják azokat. Ezen 40 millió jármű között számtalan olyan jármű lehet, amely pontos útvonalának, illetve geolokációs adatainak ismerete akár nemzetbiztonsági kockázatot is hordozhat, például védett személyek szállítására használt eszközök, kormányzati és veszélyes anyagot vagy kurrens árut[34] szállító járművek. Egy gépjárműadatokkal foglalkozó cég munkatársa elmondta az üggyel kapcsolatban, nem hiszi, hogy valóban anonimizálni lehetne ezeket az adatokat anélkül, hogy teljesen meg legyenek változtatva és el ne veszítsék az értéküket.

Az ENISA azt javasolja, hogy minden egyes IoT-környezet esetében kockázatértékelést kell végezni, módszeresen megvizsgálva a különböző eszközöket érintő fenyegetéseket, és meg kell határozni a valószínűsíthető támadási forgatókönyveket. Miután ez megtörtént, akkor el kell dönteni, melyek a kritikus és melyek a nem kritikus veszélyek az adott IoT-rendszer (eszköz) szempontjából, és melyek azok, amelyek mérsékelhetők, illetve a mérséklés érdekében milyen eszközöket és eljárásokat célszerű igénybe venni.

A létfontosságú infrastruktúrák vonatkozásában már készültek olyan előzetes tudományos felmérések és tanulmányok, amelyek bemutatják a létfontosságú

---

31 https://otonomo.io/ (Letöltés ideje: 2022. 02. 21.)

32 non-descript identifier

33 Cox, Joseph: 'Privacy Protecting' Car Location Data Seemingly Shows Where People Live Work, and Go; 2021. június 10, https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo (Letöltés ideje: 2022. 02. 21.)

34 Például üzemanyagot, vakcinát, gyógyszereket, vérkészletet, emberi szervet stb.

infrastruktúrákban elhelyezett IoT-eszközök kockázatait. Dr. Krasznay Csaba ezt részletesebben is tárgyalja *Okoseszközök a kritikus információs infrastruktúrákban* című művében, valamint ebben előre vetíti az IPAR4.0 és az IoT-eszközök kapcsolatrendszerében rejlő kockázatokat.[35]

IoT-ökoszisztéma és annak kockázatai

Annak érdekében, hogy tudjuk azonosítani egy IoT-rendszer kockázatait, ismernünk kell az ilyen rendszerek felépítését.

Az IoT-környezetekben az eszköz olyan fizikai vagy virtuális tárgy, amely egyedileg azonosítható és integrálható a már meglévő kommunikációs hálózatokba, és amelynek mindenképpen képesnek kell lennie hálózaton keresztül adatcserére egy másik eszközzel vagy rendszerrel és/vagy felhőalapú szolgáltatással. Ezen eszközök nem csak az adatcsere szempontjából érdekesek a kockázatkezelés során, hanem amiatt is, hogy ma már ezek az eszközök lehetnek olyan komplex eszközök is, amelyek tárolják, és egyben feldolgozzák, vagy akár titkosít(hat)ják is az adatokat.

Az IoT-ökoszisztéma fontos elemei az érzékelők is, mivel ezek szerves részét képezik annak a környezetnek, illetve azon környezet megfigyelésének, amelyben az IoT-rendszereket használjuk[36].

A beágyazott IoT-eszközök nemcsak érzékelő és/vagy működtető eszközöket tartalmaznak, hanem olyan egységeket is, amelyekkel közvetlenül más hálózathoz (főképpen helyi hálózathoz[37]) vagy a felhőhöz tudnak csatlakozni, memóriaterülettel és szoftverfuttatási képességgel is rendelkeznek, valamint képesek önálló adatfeldolgozásra. Ilyen eszközök például a viselhető eszközök, az intelligens termosztátok, illetve a házautomatizálási rendszerek nagy része.

Resperger István szerint[38] a kockázatok az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. A kihívás alacsonyabb szintű állapot, míg a fenyegetés a legmagasabb szintű, amikor már nemzeti érdekek sérülhetnek. Napjainkban az IoT-ökoszisztémák nemzetbiztonsági kockázati tényezői értelmezhetetlenek nemzetállami léptékekben, csakis globális szintű megközelítés és kezelés vezethet eredményre. A nemzetbiztonság szempontjából növekvő kockázatot jelentenek például:

– az eltérő társadalmi fejlődésből fakadó, országok és csoportok közötti, átmeneti vagy tartós ellentétek,

---

35 TÖRÖK Bernát: Információ és kiberbiztonság; Fenntartható biztonság és társadalmi környezet tanulmányok, V. Budapest, 2020. p. 121.

36 Ezek az érzékelők fizikai szinten fizikai, kémiai vagy biológiai mutatókat mérhetnek, digitális szinten pedig a hálózatról és alkalmazásokról gyűjtenek információkat.

37 LAN – local area network

38 RESPERGER István: Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig; Felderítő Szemle, 2013/3. p. 5.; RESPERGER István: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során; Doktori értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2002. p. 45.

- a gazdasági, pénzügyi és társadalmi különbségek okozta válságok,
- az etnikai és vallási feszültségek,
- a terrorizmus,
- a szervezett bűnözés és a közbizalmat aláásó bűncselekmények (pld. a korrupció, rémhírterjesztés stb.),
- az illegális kábítószer- és fegyverkereskedelem valamint embercsempészet,
- a tömeges migráció,
- a környezeti szennyezések és egyéb környezeti hatások,
- a tömegpusztító fegyverek és azok hordozóeszközeinek elterjedése,
- az információs rendszerek elleni támadások, valamint,
- a járványok (pl. Covid19[39]) nemzetbiztonsági kockázata.

Az internet használatának általánossá válása, majd az IoT-ökoszisztémák megjelenése a nemzetbiztonsági kockázatokat is átértelmezte – míg régebben a terroristához a szélsőséges politikai vagy vallási nézeteket valló, netalán szeparatista, mindenre elszánt harcos sztereotípia kapcsolódott, ma már a zsaroló vírussal vagy rosszindulatú kóddal operáló, stratégiai fontosságú szervezeteket megtámadó hackerek is terrorista besorolást kapnak az Amerikai Egyesült Államokban.

Az IoT-világ rohamos bővülése – éppen ezért – rákényszeríti a nemzetbiztonsággal foglalkozó szakembereket a kockázatkezelés újabb és újabb formáinak kidolgozására. Ma már sokkal kisebb az esélye egy olajfinomító vagy atomerőmű megtámadásnak helyszíni fizikai beavatkozással, mint az, hogy távolról a kapcsolódó hálózatok segítségével manipulálják a rendszereket a kiberbűnözők. Az informatikai hálózatok interdiszciplináris jellege miatt távolról is elérhető a létfontosságú infrastruktúrák rendszere, így nem zárható ki, hogy a támadók nem találnak belépési lehetőséget a rendszerbe, egy-egy hátsókapu kihasználásával pedig komoly károkat képesek okozni akár nemzetgazdasági szinten is. Volt már arra is példa, hogy egy kaszinót a beltérben elhelyezett akvárium hőmérőjén keresztül „rabolták ki”, így a támadóknak elég csak elolvasniuk egy adott ország információbiztonságra vonatkozó elsődleges jogforrását,[40] és annak hatályából már ki is derül, melyek azok az szervezetek, amelyeket az adott ország félt[41] – a törvényhozástól és a végrehajtó hatalom intézményeitől kezdve a bankokon át egészen az online piacterekig.

Nemzetbiztonsági kockázatok

A GDPR adatvédelemre és adatbiztonságra vonatkozó szabályozásával foglalkozni kell akkor is, ha egy adott szervezetben jellemzően az Infotv. hatálya alá tartozó nemzetbiztonsági célú adatkezelés folyik, mivel nemzetbiztonsági kockázatot nemcsak az az adatkezelés hordozhat, amely a nemzetbiztonsági és honvédelmi

[39] A Covid19 a súlyos akut légzőszervi szindróma-koronavírus (SARS-CoV-2) nevű vírus által okozott betegség. A SARS-CoV-2 a koronavírus egy új törzse. A vírust 2019 decemberét megelőzően nem azonosították emberekben.

[40] Magyarország: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (Letöltés ideje: 2022. 02. 22.)

[41] Ibtv. 2§

adatkezelések nagy halmazába tartozik, hanem sok más, akár a GDPR hatálya alá tartozó adatkezelés is. Az intelligens utakra, a repülőterekre, a kórházakra, a pénzintézetekre, a kommunikációs hálózatra, vagy éppen a vasútra például alapvetően a GDPR vonatkozik, ettől függetlenül ezen infrastruktúrák számos olyan kockázatot hordoznak magunkban, amelyek a nemzetbiztonsági kategóriába tartoznak. Ezen kívül az Infotv. hatálya alá tartozó adatkezelések esetében is – bizonyos esetekben – segítségül hívható a GDPR jogértelmezési gyakorlata, például olyan területeken, mint a személyes adat fogalma:

„Személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.[42]

1. érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;

1a. azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

2. személyes adat: az érintettre vonatkozó bármely információ.[43]

A GDPR adatvédelmi logikájának ismerete azért is fontos az IoT-eszközök nemzetbiztonsági kockázatkezelési célú vizsgálata során, mert ugyanazzal az eszközzel folytatott adatkezelés – az eszköz éppen aktuális felhasználásától függően – a GDPR és az Infotv. hatálya alá is tartozhat, valamint az egyértelműen a GDPR hatálya alá tartozó adatkezelésnek (illetve az adatkezelésre használt IoT-eszköznek, rendszernek) is lehet nemzetbiztonsági kockázata[44]. Így például számos új IoT-eszköz rejt nemzetbiztonsági kockázatot a Virtual Voice Assisstant alkalmazásának köszönhetően, mivel az ezzel felszerelt eszközök akár távolról beindítható lehallgató funkcióval is üzemeltethetőek, miközben az adott tárgy tulajdonosa, illetve az eszköz hatókörében tartózkodó egyéb személyek (érintettek) nem biztos, hogy tudatában vannak annak, hogy lehallgatják őket.

A teljesség igénye nélkül a fokozottan kockázatos IoT-eszközök körébe sorolhatók például:

- otthoni munkavégzéshez szükséges technika (PC, laptop, tablet, telefon, nyomtató, rajztábla stb.);
- az okos játékok (RC[45]-járművek, okosbaba, okos játékkonyha, okos babaház, játékkonzolok stb.);

---

[42] GDPR 4. cikk 1. pont

[43] Infotv. 3.§

[44] Például honvédelmi célú kapcsolódó jármű intelligens úton haladva kommunikál a környezetében lévő járművekkel és infrastruktúrákkal, járvány idején a kórházakba kirendelt katonák szolgálatteljesítésük közben rákapcsolódnak a kórház IoT-ökoszisztémájára stb.

[45] radio control

- polgári UAV[46]-rendszerek (pld. klasszikus értelemben vett drónok);
- okos otthon eszközök („smart home”);
  - háztartási gépek, eszközök (okos hűtő, mosogatógép, mosógép, sütő, vízforraló, páraelszívó stb.),
  - takarító és egyéb eszközök (okos porszívó, okos önjáró porszívó, légtisztító rendszer vagy önálló állomás stb.),
  - szórakoztató elektronika (okos televízió, hangfalrendszerek, fejhallgató stb.),
  - biztonsági eszközök (elektronikus megfigyelőrendszer, videós kaputelefon, riasztórendszer, okos zár és a biztonsági rendszerhez kapcsolódó szenzorok pld. nyitásérzékelő, infrasorompó stb.),
  - okos használati tárgyak (kuka, ágy, redőny stb.),
  - személyi egészségügyi szenzorral, biometrikus adatrögzítéssel ellátott eszközök (sportóra, véroxigén-mérő eszköz stb.),
  - lakás energetikai hálózat eszközei (hőmérséklet- és páratartalom-szabályzók és szenzorjaik, aljzatok és kapcsolók, fogyasztásmérők, automatizált árnyékolók stb.),
  - testre szabható világítástechnika (stacioner lámpák és szenzorjai, asztali lámpák, okos izzók, mozgásérzékelővel ellátott éjjeli fények, LED világítás vezérlés és szenzorjai stb.),
  - személyi higiéniai eszközök (fogkefe, arcápolási termékek stb.),
  - kerti és hobbi eszközök (okos fűnyíró, öntözőrendszer, intelligens szerszámok, uszodatechnika stb.),
  - házi állatokhoz tartozó eszközök (ételadagoló rendszerek, akvárium hőmérő, kisállatra szerelhető szenzorok, játékok, kiképző eszközök stb.);
- személyi viselhető okoseszközök (szemüveg, óra, GPS-pozíció meghatározására alkalmas eszközök, okos ruházat és kiegészítők, pld. kulacs, cipő stb.);
- kapcsolódó járművek (személygépkocsikba, egyéb járművekbe telepített IoT-eszközök).

A legkülönfélébb eszközök kockázatát növeli a készülékekbe integrált hangasszisztens, illetve a különböző egészségügyi és biometrikus adatokat kezelő alkalmazások.

Összességében megállapítható, hogy a technológiai újítások megjelenése,[47] illetve a már meglévő eljárásokban rejlő nemzetbiztonsági kockázatok,[48] valamint a személyes adatok (pld. kép- és hangfelvétel) biometrikus adatokként felhasználása a hatályban lévő jogszabályok alapelveinek újraértelmezésére kényszeríti mind az Alapjogi Chartát tiszteletben tartani kívánó adatkezelőket, mind a jog érvényesítésére törekvő felügyeleti hatóságokat és bíróságokat. A helyzetet tovább bonyolítja, hogy bizonyos személyes adatokkal kapcsolatos adatkezelések nem tartoznak a GDPR hatálya alá, így ezekben az esetekben a vonatkozó jogszabályok értelmezése a nemzeti hatóságok feladata, illetve bűnügyi adatok kezelése esetében a bűnügyi adatvédelmi

[46] pilóta nélküli repülőgép – Unmanned Aerial Vehicle – UAV
[47] mesterséges intelligencia, gépi tanulás, nagy adat, blokklánc
[48] arcfelismerő rendszerek, érzelemfelismerő, lelkiállapotot monitorozó applikációk

irányelv hatálya alá tartozó adatkezelésekkel kapcsolatban az Európai Adatvédelmi Testület is bocsáthat ki iránymutatást és véleményt.

A téma kutatásakor mindenképpen érdemes figyelembe venni a 29. cikk szerinti Adatvédelmi Munkacsoport 2014-es véleményét, amely szerint, *„a tárgyak internete azon az elven alapul, hogy hatalmas mennyiségű adatot kezeljenek (…) A tárgyak internetében részes érdekeltek célja, hogy az egyénekre vonatkozó ilyen adatok további kombinálásával új alkalmazásokat és szolgáltatásokat kínáljanak – akár azért, hogy „csak" a felhasználó környezet-specifikus adatait mérjék, akár azért, hogy konkrétan megfigyeljék és elemezzék a szokásait. Más szóval: a tárgyak internete általában olyan adatok kezelését jelenti, amelyek azonosított vagy azonosítható természetes személyekre vonatkoznak, és ezért az uniós adatvédelmi irányelv 2. cikke értelmében*[49] *személyes adatoknak minősülnek"*[50].

A ma már szinte „ősréginek" számító munkacsoport-vélemény három területet jár körbe részletesen, úgymint:

- testen hordható számítástechnikai eszközök,[51]
- a számszerűsített én („Quantified Self[52]") és
- az otthonok automatizálása,

a megállapításai pedig mind a mai napig irányadóak.

A számszerűsített énnel kapcsolatban a vélemény külön foglalkozik a különböző típusú adatokkal[53], kiemelve az IoT-eszközök azon tulajdonságát, miszerint az eszközök egy részén csak a megjeleníthető adatok jelennek meg a felhasználó számára, miközben az eszköz ennél akár jóval több adatkategóriában is gyűjthet adatot. A program készítője általában az eszközön megjelenített adatkörnél sokkal több adathoz férhet hozzá, amelyeket a későbbiekben akár úgy is elemezhet, illetve más adatbázisokkal összevethet, hogy arról az érintettnek nincs tudomása, sőt akár még kereskedhet is ezekkel az adatokkal. Ez a jelenség 2021 folyamán is több olyan esetben jelent meg a médiában, ahol ezt a másodlagosan megküldött adatelemzést komoly kockázatnak minősítették[54]. Ez a módszer az IoT-verziója annak, amikor informatikai eszközökre telepített szoftverek többletinformációkat továbbítanak a gyártó/fejlesztő, illetve azok különböző partnerei részére a felhasználó tudta nélkül.

---

[49] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=DE (Letöltés ideje: 2022. 02. 21.)

[50] WP233, 4. o.

[51] Okos óra és okos szemüveg.

[52] A számszerűsített én mind a technológiával történő önkövetés kulturális jelenségére, mind az önkövető eszközök felhasználói és készítőinek közösségére utal.

[53] Nyers adatok, összesített adatok és kinyert információ, valamint a megjeleníthető adatok.

[54] A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers; An FTC Staff Report, October 21, 2021, https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf (Letöltés ideje: 2022. 02. 21.)

A vélemény által felsorolt kihívások mind a mai napig kockázatokat hordoznak, így többek között:

- az IoT-eszközök esetében jellemző a felhasználói kontrol hiánya és az információs aszimmetria, amely azt eredményezi, hogy az érintett elveszítheti a rendelkezést a saját adatai felett. A probléma súlyát jelzi, hogy az Unióban a legtöbb adatvédelmi bírságot az érintettek tájékoztatásának (transzparencia) hiánya miatt szabják ki, illetve a vállalkozások mind a mai napig nem hagytak fel az adatok jogszerűtlen felhasználásával;[55]
- A felhasználó tudta nélkül kezelik személyes adatait. Kiemelt nemzetbiztonsági kockázatot jelentenek például azok az okos órák, amelyek megtévesztésig hasonlítanak a nem digitális órákra, miközben beágyazott mikrofonnal és kamerával rendelkeznek, azaz bárkiről annak tudtán kívül felvételeket készíthet. Ugyanez a probléma más viselhető eszközökkel is, például az okos szemüveggel, és más, nem testkamerának kinéző testkamerával, a helyzet súlyosságát pedig az is jelzi, hogy 2021 decemberében Németországban külön hatósági figyelmeztetés jelent meg arra vonatkozóan, hogy az ilyen ún. „kémeszközök" alkalmazása tiltott:[56]
  „A fogyasztóknak e termékek vásárlásakor különösen a következőkre kell figyelniük
  1. *Van a termékben vezeték nélküli kamera vagy mikrofon?*
  2. *A kép- vagy hangfájlokat vezeték nélkül továbbítják-e harmadik félnek anélkül, hogy a rögzített személynek erről tudomása lenne, vagy hogy a rögzítési helyzetet ellenőrizni tudná?*
  3. *A mikrofonhoz vagy a kamerához rejtett módon kívülről is hozzá lehet férni? Mindezen esetekben a termék tiltott."*;
- Az érintetteknek gyakran nincs ráhatásuk arra, hogy az adataikból nyert következtetések és az eredeti adatkezelés egyéb célra történő felhasználása mi célt szolgál. Így például az okostelefon gyorsulásérzékelőjével és forgásmérőjével eredetileg gyűjtött, az érintett számára látszólag jelentéktelen adatok felhasználhatók arra, hogy az egyén vezetési szokásait elemezzék;
- A profilozás lehetősége a „Big Data" korszakában új távlatokat kapott, egy adott személy élete a mobiltelefonján/okosóráján keresztül szinte tökéletesen összerakható és kielemezhető, ráadásul ezen alkalmazások keretében különleges adatok is megosztásra kerül(het)nek. És mindez úgy, hogy az érintettnek fogalma sincs minderről, ráadásul megfelelő tájékoztatás hiányában lépéseket sem tud tenni a profilozásának megelőzése, befolyásolása, illetve megszüntetése érdekében, mindennek az

---

[55] „Agresszív" adatgyűjtés miatt kapott bírságot az Apple és a Google; https://nki.gov.hu/it-biztonsag/hirek/agressziv-adatgyujtes-miatt-kapott-birsagot-az-apple-es-a-google/ (Letöltés ideje: 2022. 02. 21.)

[56] Bundesnetzagentur empfiehlt Vorsicht beim Kauf von smarten Produkten als Weihnachtsgeschenk, Pressemitteilung, Bonn, 20. 12. 2021, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2021/20211220_Smart.pdf;jsessionid=A12415C4E8C492B79A164A86968C316C?__blob=publicationFile&v=https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2021/20211220_Smart.pdf;jsessionid=A12415C4E8C492B79A164A86968C316C?__blob=publicationFile&v=2 (Letöltés ideje: 2022. 02. 21.)

eredménye pedig akár egy kafkai univerzumba csöppenés[57] érzete is lehet. Mindeközben az adatkezelők anonimizálásra hivatkozva adják-veszik ezeket az adatokat, amelyek aztán a későbbiekben a legmodernebb algoritmusoknak köszönhetően újra személyhez köthetőek;[58]

- Az IoT-eszközök alkalmazása jelentősen befolyásolja az internetes anonimitás kérdését. A folyamatos megfigyelés egyfajta Big Brother[59] illúziót kelthet, amelynek szintén erőteljes frusztrációs hatása lehet az egyén számára, az új technikai megoldások pedig a „felügyeleti kapitalizmus" térhódítását segítik.[60] Emellett IoT-eszközeink egy része akarva-akaratlanul is kötődik hozzánk, mivel ez feltétele üzemszerű működésüknek (személykövető GPS-eszközök);
- A kevésbé biztonságos IoT-eszközök potenciálisan hatékony támadási módokat eredményezhetnek, mivel a megfigyelési módszereket egyszerűsíthetik, illetve a személyes adatok ellopását is elősegítik. Maga az IoT-eszköz biztonsága mellett[61] a kommunikációs kapcsolatok és a tárolóinfrastruktúra biztonsága is kiemelt szempont, különös tekintettel az önkövető rendszerek biztonsági hibáira (pld. lépésszámláló, alvásmonitor), mert ezek megfigyelt értékeinek meghamisítása súlyos kockázatot jelenthet az érintett életére (például téves értékekre tekintettel hozott döntés stb.);
- A tárgyak internetének keretében automatikusan kezelt nagy mennyiségű anonimizált adat az újraazonosítás kockázatát vonja maga után. Ilyen volt például az a 2013-as eset,[62] amikor a New York-i Taxi és Limuzin Bizottság közzétett egy adatbázist, amelyben több mint 173 millió egyéni taxifuvarral kapcsolatban volt megadva a be- és kiszállás helye, időpontja és az „anonimizált" engedélyszámok. Azonban az adatbázis nem volt megfelelően anonimizálva, ennek köszönhetően nemcsak az eredeti engedélyszámokat lehetett azonosítani, hanem az egyes taxisofőröket is;
- A 29. cikk szerinti Adatvédelmi Munkacsoport 2014-es figyelmeztetése az eltelt pár év alatt csak hangsúlyosabb lett, 2021-ben pedig a spanyol adatvédelmi hatóság (AEPD[63]) és az Európai Adatvédelmi Biztos (EDPS[64]) közös kiadványban[65] mutatta be az anonimizálással kapcsolatos tíz

---

57 KAFKA, Franz: A per (1914); https://mek.oszk.hu/07100/07123/07123.htm (Letöltés ideje: 2022. 02. 21.)

58 SHERMAN, Justin: Big Data May Not Know Your Name. But It Knows Everything Else, 12. 19. 2021. https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/ (Letöltés ideje: 2022. 02. 21.)

59 ORWELL, George: 1984; Harcourt Brace, New York, 1949.

60 ZUBOFF, Shoshana: The Age of Surveillance Capitalism: The Fight For a Human Future At the New Frontier of Power; Public Affairs, New York, 2019, ISBN 9781610395700

61 BBC: Alexa tells 10-year-old girl to put penny in plug socket; 2021. december 28., https://www.bbc.com/news/technology-59810383 (Letöltés ideje: 2022. 02. 21.)

62 PANDURANGAN, V: On taxis and rainbows: Lessons from NYC's improperly anonymized taxi logs; 2014. https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a (Letöltés ideje: 2022. 02. 21.)

63 Agencia Española de Protección de Datos

64 European Data Protection Supervisor

65 AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation; https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en (Letöltés ideje: 2022. 02. 22.)

legelterjedtebb tévhitet, és ezen a téren a hazai gyakorlat sem mindig tökéletes;[66]

- Az alkalmazásfejlesztők harmadik félként jelenhetnek meg, így nemcsak a készülék gyártója, hanem harmadik félként az alkalmazásfejlesztő is hozzáfér az adatokhoz, miközben az ezzel kapcsolatos tájékoztatás gyakran meglehetősen hiányos, de akár teljesen hiányozhat is – elég csak elolvasni egy modern gépjármű csatlakoztatott, modemes applikációjának ajánlását:
- *„Információt biztosít mindenről, az utazás útvonalának optimalizálásától az öndiagnosztikán át egészen a jármű állapotára vonatkozó figyelmeztetések küldéséig, az elektromos jármű töltőpontok megkereséséig, valamint a jármű teljes feltöltéséről való tájékoztatásig. (…) Az Utazások funkció a háttérben a tartózkodási helyet használja az útvonalak és más kulcsfontosságú vezetési események rögzítésére, hogy betekintést nyújtson vezetési szokásaiba."*[67];
- Az adatokat feldolgozó egyéb, harmadik fél is megjelenhet az IoT-rendszerekben, ilyen lehet például a biztosító, amikor lépésszámlálót/sportórát ad a biztosítottnak, annak érdekében, hogy a díjat az ügyfele életmódjához tudja igazítani.

Az IoT-eszközök nemzetbiztonsági kockázatainak feltárása esetén a kockázat értékelése minden esetben egyedi mérlegelést igényel, azaz esetről-esetre egyedileg kell felmérni, van-e az adott eszközzel vagy rendszerrel kapcsolatban nemzetbiztonsági kockázat, és ha van, milyen intézkedésekkel lehet azt csökkenteni.

Vannak azonban olyan eszközök, amelyek alapvetően magukban hordozzák a nemzetbiztonsági kockázatot, bárkinél is vannak, bármire is használják azokat. Ilyen eszközök/rendszerek például az IoMT-[68] és IoBT[69]-eszközök, amelyek többsége eleve korlátozott forgalmú eszköz. A mindennapi életben használt IoT-eszközök többségének nemzetbiztonsági kockázata azonban nem a puszta létéből fakad, hanem abból, hogy ki, mikor, hol és mire használja, valamint ki fér hozzá az adatokhoz.

Kiemelt nemzetbiztonsági kockázati tényező lehet például olyan IoT-eszköz, amelyről a felhasználó sem tudja, hogy az. Egy okos gyermekjátéknak polgári környezetben nem értékelhető a nemzetbiztonsági kockázata. Ha ugyanez az eszköz egy katonai objektum parancsnokának gyermekéhez tartozik, akkor viszont akár kritikus is lehet, mivel bekerülhet az illetékes parancsnok objektumába. Emellett a gyerekek – életkoruknál fogva – nem tudják, hogy mivel állnak szemben, így olyan adatokat oszthatnak meg a játékukkal (és a játékok által használt alkalmazásokkal), amelyek egy, például a játékgyártó vagy a felhőszolgáltató rendszerét érintő

---

66 Hvg.hu: Nagyot kockáztattak a magyar hatóságok a Szputnyik V vakcinával az OGYÉI dokumentumai szerint; 2021. december 23. https://hvg.hu/tudomany/20211223_szputnyik_v_vakcina_ogyei_dokumentumok_hadhazy_akos (Letöltés ideje: 2022. 02. 22.)

67 Ford Motor Co: FordPass; https://play.google.com/store/apps/details?id=com.ford.fordpasseu&hl=hu&gl=US (Letöltés ideje: 2022. 02. 22.)

68 Internet of Military Things

69 Internet of Battlefield Things

adatvédelmi incidens esetén akár rosszkezekbe is kerülhetnek[70,71]. Rosszabb esetben képek és hangfelvételek is kikerülhetnek az objektum belsejéről, a beléptető rendszer egyes paramétereiről, az őrség mozgásáról stb.

Az okoseszközök nemzetbiztonsági kockázata is attól függ, ki használja – az eszköz nemzetbiztonsági kockázata nagyságrendekkel nagyobb akkor, ha szervezett bűnözésben érdekelt személyek használják kommunikációra titkosító applikációk segítségével az adott eszközt, és más akkor, ha egyetemisták beszélik meg rajta a következő csoportprojekt feladatait. Ez a kockázat jelentősen csökkenthető abban az esetben, ha a hatóságok által feltörhető, a szervezett bűnözői csoport által viszont feltörhetetlennek hitt alkalmazásokon keresztül történik a kommunikáció. Az okostelefon – mint az egyik legkomplexebb IoT-eszköz – kockázata attól is függ, hogy mire használják. Az okostelefon – jelentősen növelve használatának kockázatát – akár teljes értékű POS-terminálként is tud működni. Immáron Magyarországon is elérhető a myPOS-szolgáltatónak az a technológiája, amelynek köszönhetően egy Android rendszerű telefon alkalmassá tehető érintéses NFC-fizetések fogadására.

A kiberbiztonsági szakemberek azzal is tisztában vannak, hogy a szolgálati célú okostelefonnal rendelkező állomány tagjai – hibás konfigurálás esetén – akár akaratlanul is telepíthetnek olyan alkalmazást az eszközeikre, amely komoly kockázati tényezővel rendelkezik. Mindez komoly nemzetbiztonsági problémát hordozhat, különösen akkor, ha ellenérdekelt nemzetbiztonsági szolgálat figyeli meg a készüléket. A tapasztalatlan szolgálati okostelefon-használók pedig még tovább fokozva a kockázatot, akár illegális módszerekhez folyamodva, „továbbfejleszthetik" a készülékeket[72].

A használat helyszíne is nagyban befolyásolhatja a nemzetbiztonsági kockázat szintjét, más kockázattal bír egy internetre kötött kávéautomata egy polgári vállalkozásnál és mással akkor, ha egy hadműveleti központ közelében telepítették. A használat időpontja is növelheti a nemzetbiztonsági kockázatot, mivel egyébként „ártalmatlan" IoT-rendszerek akár jelentős többletkockázattal is bírhatnak például természeti katasztrófa vagy járvány pusztítása idején (pl. rémhírterjesztésre használva az okostelefont/drónt stb.)

A közelmúlt kiberbiztonsági eseményei rámutattak arra, hogy a kiberbűnözők jelentős károkat tudnak okozni az internetre csatlakoztatott rendszerek támadásával. Az amerikai kormány rövid idő alatt három jelentős kiberbiztonsági incidenssel is kénytelen volt szembenézni (Solarwinds eset[73], a Colonial Pipeline vezetékhálózat

---

70 Név, lakcím, életkor, kedvenc kutya-macska neve, felvételek a gyerekekről, a lakásról, hozzátartozókról és bárkiről/bármiről, aki/ami csak előfordul a gyermek környezetében.

71 Például: Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act, January 8, 2018. https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated (Letöltés ideje: 2022. 02. 22.)

72 rooting, jailbreaking

73 Nemzeti Kibervédelmi Intézet: A Solarwinds incidens, Kiberbiztonsági elemzés; https://nki.gov.hu/wp-content/uploads/2021/09/NBSZ-NKI-Kiberbiztons%C3%A1gi-elemz%C3%A9s-a-SolarWinds-incidensr%C5%91l.pdf (Letöltés ideje: 2021. 02. 22.)

elleni támadás és a JBS élelmiszeripari incidens[74]), korábban pedig egy kőolajfinomító elleni támadás (Szaúd-Arábia,) és az ivóvíz távolról történő megmérgezése (Ukrajna) demonstrálta, hogy a támadóknak az emberi életek elvesztése sem okoz lelkiismereti problémát. A Colonial Pipeline támadás komoly ellátási zavarokat okozott (akár zavargásokhoz is vezethetett volna), a JBS-ügy ráadásul nem maradt meg nemzetállami szinten, hanem érintette Kanadát és Ausztráliát is. Ezek az esetek bemutatták, hogy egy kis hackercsoport – akár megrendelésre is – megfelelő civil célpont megtámadásával erős országokat is „térdre kényszeríthet", mégha csak időlegesen is.

Az okos rendszerek térhódításával az IoT-világ nemzetbiztonsági kockázata egyre nagyobb lesz, gondoljunk csak olyan rendszerekre, mint például az intelligens város, repülőtér, kikötő, vasút-, közút- és energiahálózat. Ezek stratégiai szerepe mind nemzeti, mind globális szinten jelentős, az összekapcsolódásuk és egymástól függésük egyre interdiszciplinárisabb problémákat fog felszínre hozni, az információbiztonság pedig egyben nemzetbiztonsági kérdés is lesz, különös tekintettel a veszélyeztetett életekre, és az ország, valamint a gazdaság biztonságára.

Az IoT-eszközök ráadásul számtalan olyan személyes adatot kezelhetnek, amelyek nemzetbiztonsági szempontból kockázatos adatkezelésekkel kapcsolatosak. Az, hogy egy adott adatkezelés mely jogszabály hatálya alá tartozik, azt mindig az adatkezelés célja határozza meg, így az Infotv. hatálya alá tartoznak a bűnüldözési,[75] nemzetbiztonsági,[76] illetve honvédelmi[77] célú adatkezelések, a jogszabály pedig az értelmező rendelkezések keretében definiálja ezeket a célokat. Az Infotv. hatálya alá tartoznak például a gyülekezési törvény hatálya alá tartozó

---

74 Reuters 2021. június 10. https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/ (Letöltés ideje: 2022. 02. 22.)

75 Infotv. 3.§ 10a. pontja alapján bűnüldözési célú adatkezelés: a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy ezen tevékenység keretei között és céljából – ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is – végzett adatkezelése.

76 Infotv. 3.§ 10b. pontja alapján nemzetbiztonsági célú adatkezelés: a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelése, valamint a rendőrség terrorizmust elhárító szervének jogszabályban meghatározott feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelése.

77 Infotv. 3.§ 10c. pontja alapján honvédelmi célú adatkezelés: a honvédségi adatkezelésről szóló törvény, továbbá a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló törvény, és a Magyar Köztársaság területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyar Köztársaság területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról, valamint jogállásukhoz kapcsolódó egyes rendelkezésekről szóló törvény hatálya alá tartozó adatkezelés.

rendezvénybiztosításokkal[78] és a büntetőeljárás lefolytatásával[79] kapcsolatos adatkezelések, valamint a körözött személyek nyilvántartása[80] is.

A GDPR hatálya alá tartozik – leegyszerűsítve – mindaz, ami nem tartozik az Infotv. hatálya alá, például a VÉDA-kapukkal[81] és az objektív felelősséggel kapcsolatos adatkezelések,[82] a rendőrök (szolgálati jogviszonyban lévők) személyügyi adatkezelései[83] és a rendvédelmi alkalmazottak személyügyi alapnyilvántartása[84]. Ha valakinek pedig kétsége lenne, hogy ezen adatkezelések besorolása a GDPR alá megfelelő-e, akkor irányadónak veheti azt az esetet, amikor a NAIH a GDPR rendelkezéseinek megsértése miatt büntette meg ötmillió forintra a Budapesti Rendőr Főkapitányságot (BRFK), mert annak munkatársa egy olyan adathordozót hagyott el, amelyen 1733 fő rendvédelmi alkalmazotti jogviszonnyal érintett személy személyes adata volt.[85] Iránymutatásul szolgálhat továbbá az Infotv. és a GDPR hatályával kapcsolatos NAIH-állásfoglalás is, amely a büntetésvégrehajtás adatkezeléseivel kapcsolatos.[86]

A GDPR hatálya alá tartozik a rendőrök szolgálati gépjárművel munkavégzésének ellenőrzése a Jármű Követő Rendszeren (JKR[87]) keresztül,[88] amely

[78] ORFK érintetti tájékoztató. Gyülekezési törvény hatálya alá tartozó rendezvénybiztosítások; http://www.police.hu/sites/default/files/2019-06/kozrendvedelem_148_v1.1_0.pdf (Letöltés ideje: 2021. 02. 22.)

[79] ORFK érintetti tájékoztató. Büntetőeljárás; http://www.police.hu/sites/default/files/2020-10/bunugy_049_v1.3.pdf (Letöltés ideje: 2022. 02. 22.)

[80] ORFK érintetti tájékoztató. Körözött személyek nyilvántartása; http://www.police.hu/sites/default/files/2020-10/bunugy_245_v1.3.pdf (Letöltés ideje: 2022. 02. 22.)

[81] ORFK érintetti tájékoztató. A VÉDA Közúti Intelligens Kamerahálózat általi adatok kezelése és továbbítása; http://www.police.hu/sites/default/files/2020-03/V%C3%89DA%20%C3%A9rintetti%20t%C3%A1j%C3%A9koztat%C3%B3.pdf (Letöltés ideje: 2021. 02. 22.)

[82] ORFK érintetti tájékoztató. Objektív felelősséggel kapcsolatos közigazgatási hatósági ügyek; http://www.police.hu/sites/default/files/2020-03/Kktv.%2021.%20%C2%A7%20objekt%C3%ADv%20felel%C5%91ss%C3%A9g%20%C3%A9rintetti%20t%C3%A1j%C3%A9koztat%C3%B3%20.pdf (Letöltés ideje: 2022. 02. 22.)

[83] ORFK érintetti tájékoztató. Személyügyi nyilvántartás; http://www.police.hu/sites/default/files/2019-06/humanigazgatas_223_v1.1_0.pdf (Letöltés ideje: 2022. 02. 22.)

[84] ORFK érintetti tájékoztató. Rendvédelmi alkalmazottak személyügyi alapnyilvántartása; http://www.police.hu/sites/default/files/2019-08/humanigazgatas_255_v1.0.pdf (Letöltés ideje: 2021. 02. 22.)

[85] NAIH/2019/2471/6. sz. határozat. Döntés hivatalból induló adatvédelmi hatósági eljárásban; 2019. június 25. https://naih.hu/files/NAIH-2019-2471-hatarozat.pdf (Letöltés ideje: 2022. 02. 22.)

[86] NAIH-5728- /2021.

[87] https://www.police.hu/adatvedelmi-tajekoztatok/hu!a-rendorsegrol!adatvedelem!altalanos-ugytipusok!allomannyal-kapcsolatos-adatkezelesek!jarmu-koveto (Letöltés ideje: 2021. 02. 22.)

[88] ORFK érintetti tájékoztató. Jármű Követő Rendszer adatkezelése (JKR); http://www.police.hu/sites/default/files/2019-12/altalanos_258_v1.0-f%C3%BCggel%C3%A9kkel.pdf (Letöltés ideje: 2022. 02. 22.)

során az alábbi adatok rögzítésére kerül sor – többek között – IoT-eszközök segítségével:

- a szolgálati gépjárműhasználathoz kapcsolódó adatok (helymeghatározó adat, három tengely szerinti gyorsulási adat),
- a JKR által előállított adatok (a jármű és ebből következően a járművet vezető személy tartózkodási helye térképes megjelenítéssel, illetve a vezetési stílus elemzés adatai, így a jármű fokozott igénybevételét alátámasztó toleranciaszintet meghaladó gyorshajtás, motorteljesítmény, gyorsulás-lassulás adat).[89]

Az Országos Rendőr Főkapitányság (ORFK) érintetteknek szóló tájékoztatója alapján tehát a JKR nemcsak a szenzorok által rögzített adatokat rendeli a személyi állomány tagjaihoz, hanem profilozást is végez a vezetési stílusuk tekintetében – a rendőrök pedig felkészülhetnek arra, hogy az ORFK idővel sokkal precízebb és több funkcióval rendelkező IoT-eszközöket is be fog szerezni annak érdekében, hogy még pontosabb képet alkothasson a szolgálati gépjárműveket használó személyi állományról.

Természetesen az ORFK-n kívül több más olyan fegyveres erő és testület van, amely – nemzetbiztonsági érdekektől vezérelve is – számtalan IoT-eszközt alkalmaz, például testkamerákat, drónokat, rejtett lehallgató eszközöket, felvételek készítésére alkalmas eszközöket stb. Ezek mind adatokat gyűjtenek nemcsak a megfigyelt személyekről, hanem azokról is, akik a megfigyelést végzik. A testkamera felvételeiből nemcsak az látszik, hogyan viselkedik az, aki éppen szemben áll a kamera viselőjével, hanem a kamerát működtető személy is profilozható.

Az IoMT- és IoBT-eszközök esetében hasonló a helyzet, ezen eszközök alkalmazója (a katona) is érintett státuszú az adatkezelésekben, így – elviekben – minden további nélkül élhet érintetti jogaival az adatkezelő felé, különösen akkor, ha például a munkavégzésének minősége a kérdés. A világsajtót bejárta például az az eset, amikor Bulgáriában NATO-hadgyakorlaton eltévedő katonák mozgását nemcsak a szervezeti egységük IoT-ökoszisztémája örökítette meg számtalan személyes adat formájában, hanem Youtube-videó formájában nyilvánosságra kerülő civil térfigyelő kamerarendszer felvétele[90] is.

Az érintetteket segíti az is, hogy egyes esetekben[91] az IoT-eszközök által szolgáltatott adatok segíthetnek komplexebb, a szervezet számára előnytelen helyzetet megnyugtatóan megoldani, bár vannak olyan adatkezelések, amelyek esetében ezen szervezeteknek nem kell arra számítaniuk, hogy az ellenérdekelt fél[92] érintetti kérelmet nyújt be. Az Infotv. hatálya alá tartozó adatkezelések esetében az érintettek gyakran kevesebb joggal rendelkeznek mint a GDPR hatálya alá tartozó adatkezelések érintettjei, ám az ilyen típusú adatkezeléseket végző szervezeteknek is

---

89 ORFK érintetti tájékoztató. Jármű Követő Rendszer adatkezelése (JKR); http://www.police.hu/sites/default/files/2019-12/altalanos_258_v1.0-f%C3%BCggel%C3%A9kkel.pdf (Letöltés ideje: 2021. 02. 22.)

90 Euronews: US special forces mistakenly assail a factory in Bulgaria, 2021. jún. 2., https://www.youtube.com/watch?v=QzJxzVvI2p8 (Letöltés ideje: 2022. 02. 22.)

91 Zaklatás, szabálytalanul foglalkoztatás, igazolójelentés alátámasztása, balesetek kivizsgálása, félresikerült akció stb.

92 megfigyelt, nyomon követett személy

fel kell készülniük arra, hogy az Infotv-ben rögzített adatvédelmi alapelveknek nekik is meg kell felelniük, még akkor is, ha bizonyos információkat nem kell kiadniuk az érintetti kérelmekre adott válaszaikban. Sőt, az adatbiztonság magasabb követelményeket is támaszt feléjük[93], a kiszivárgott adatvédelmi incidensek pedig akár nemzetközi szintű diplomáciai botrányokat is okozhatnak, illetve negatív képet mutathatnak a médiában az adott szervezetről.

A megfigyelő rendszerek kockázatértékelése komplex feladat, amire az egyik példa a siófoki mesterséges intelligenciával ellátott kameraprojekt, amelynek keretében az üdülőváros a legnépszerűbb sétányára 39 arcfelismerő funkcióval ellátott térfigyelő kamerát kíván elhelyezni úgy, hogy ezeknek a kameráknak a gyártóját[94] 2019-ben az Amerikai Egyesült Államok kormányzata feketelistára tette[95], majd 2021 márciusában az Amerikai Egyesült Államok Hírközlési Felügyelete (FCC[96]) nemzetbiztonsági kockázattá minősítette az amerikai polgárok biztonsága és védelme érdekében. Amennyiben az amerikai álláspontot vesszük figyelembe, a kamera működtetése és esetleges nem jogszerű használata, kibertámadása, valamint a különféle szervezetek általi hozzáférés hordozhat nemzetbiztonsági kockázatot. További nyitott kérdés az, hogy a rendszer üzemeltetője illetve az adatfeldolgozók (pld. a rendszer fejlesztője) mire használja a siófoki sétányon megforduló személyek (különleges) személyes adatait, és milyen egyéb adatbázisokkal köti össze az így megszerzett információkat. Ez a kockázati tényező nagyban befolyásolhatja a nemzetbiztonsági szolgálatok műveleti tevékenységét is az említett területen.

IoT IPAR 4.0 (IIoT[97]) kockázatai

Az IPAR 4.0[98,99] olyan technológiákat használ fel, mint például az M2M[100]-kommunikáció, a „Big Data”-elemzés, a robotika, a mesterséges intelligencia, a gépi tanulás, a prediktív karbantartás, valós idejű monitorozás, felhő, kiterjesztett valóság és nem utolsó sorban az IIoT-végeszközök. Az IIoT új kockázatokat és új prioritásokat is hoz az IoT-ökoszisztémában, a kockázat természete és nagyságrendje pedig jellemzően attól függ, hogy:

- milyen iparágban, illetve létesítményben van telepítve az adott rendszer[101],
- mekkora az adott létesítmény egy adott ország, régió vagy akár globális szempontból.

---

93 felhőbiztonság, üzemfolytonosságstb

94 Dahua Technology

95 Forrás: https://www.reuters.com/article/us-usa-trade-china-exclusive-idUSKBN1WM25M (Letöltés ideje: 2022. 02. 22.)

96 Federal Communications Commission

97 Industrial Internet of Things

98 Smart Manufacturing, Industrial IoT, IIoT

99 IPAR 4.0: *„paradigmaváltás a termelésben a digitalizált, integrált és intelligens hozzáadott értékláncok irányába az elosztott döntéshozatal lehetővé tétele révén olyan új kiberfizikai technológiák beépítésével, mint például az IoT”* Lásd: ENISA: Good practices for Security of Internet of Things in the context of Smart Manufacturing; November 2018. p. 12.

100 A Machine-to-Machine technológia olyan adatáramlást jelent, amely emberi közreműködés nélkül, gépek között zajlik.

101 Hadiipari objektum, atomerőmű, kőolajfinomító, vízközmű, integrált áramkör gyár stb.

Az IIoT-rendszerek kockázatát tovább fokozza a beszállítói láncok[102] összetettsége, az elemek bizalomra épülő kapcsolódása, és a lánc tagjainak különböző biztonsági szintje.

Az IIoT-eszközök felhasználásával számos kibertámadás megvalósítható, aminek következtében számos leállás is bekövetkezhet. Ugyan nem kibertámadás eredménye, de figyelmeztető jelnek tekinthető például az általános integrált áramkör (chip) hiányt, ami 2021-ben jelentős fennakadásokat okozott a gépjárműiparban – az ilyen típusú a kockázatok megjelenhetnek a későbbiekben a jelenleg fejlesztés és kialakítás alatt álló magyar hadiiparban is.

Az ENISA külön dokumentumban tárgyalja az intelligens gyártást, amely során számos, korábban nem tapasztalt kockázatra hívja fel a figyelmet az IIoT-rendszerekkel kapcsolatban: [103]

- a zárt kiber-fizikai rendszerekről az összekapcsolt kiber-fizikai rendszerekre való áttérés miatt az intelligens gyártásban kezelni kell az IIoT rendszerekre jellemző sebezhetőségi problémákat úgy, hogy az ilyen típusú rendszerek többsége nem rendelkezik kibervédelmi alrendszerrel;
- Az intelligens termelésben az összetett folyamatok sokaságát is figyelembe kell venni, különösen azért, mert a gyakorlatban a funkcionalitás és a termelési hatékonyság általában magasabb prioritást élvez, mint a kiberbiztonság;
- Az intelligens termelésben használt rendszereknek lehetővé kell tenniük a különböző szervezetek közötti együttműködést,[104] és az ebből fakadó problémákat a biztonság szempontjából is kezelni kell. Emellett a régi és új termelési rendszerek egymásra építése-vegyítése addig ismeretlen, ámde régen meglévő sebezhetőségi pontokat is aktiválhat, előre fel nem mérhető nagyságrendű kockázatot hordozva a szereplők számára;
- Az ipari vezérlőrendszerek immáron nem elszigetelt rendszerek, így új problémák kerülhetnek felszínre, mint például a bizonytalan hálózati kapcsolatok, valamint az ismert sebezhetőséggel rendelkező technológiák használata. A vállalatok csak ritkán képesek egy-egy termék minden egyes részét saját maguk előállítani, ezért harmadik felek alkatrészeire kell támaszkodniuk. Az új technológiák bevezetése új kompetenciákat kíván a termelésben részt vevőktől, hiszen mind a mérnököknek, mind a munkásoknak olyan új típusú eszközökkel és rendszerekkel kell dolgozniuk, amelyek a korábbi szakmai ismeretek mellett digitális tudást is megkövetelnek. A szereplők – célirányos oktatás hiányában – nem ismerik az adatok gyűjtésével, kezelésével és elemzésével kapcsolatos kockázatokat, és emiatt könnyű célpontjává válhatnak a támadásoknak, illetve a legjobb IoT-eszköz se töltheti be megfelelően a rendeltetését, ha rendszeresen ellopják a töltőjét, és egy másik IoT-eszközt (pld. kamerát) kell használni a probléma megoldására.

[102] supply chain

[103] ENISA: Good practices for Security of Internet of Things in the context of Smart Manufacturing, 2018 November

[104] Beszállítói láncok, vállalatcsoport cégei stb.

Az IoT-eszközök biztonsági fenyegetéseit az ENISA több szempont alapján is tárgyalta,[105] így például a megtámadott rendszerelem, a támadás kockázatának mértéke, a következmények súlyossága, illetve a rendszerelemek veszélyeztetettségének mértéke alapján.

Okos szolgáltató rendszerek

A szolgáltatások területén is megfigyelhető az IoT térhódítása.[106] Ezen rendszerek problémái alapvetően hasonlóak az ipar problémáihoz, azonban a kockázatok kitettségét fokozza, hogy napi szinten akár emberek millióival (felhasználókkal) is kapcsolatba kerülhetnek, rendkívül komplex adatstruktúrát generálva. Ezen szolgáltatások szintén erőteljesen kitettek a beszállítói láncok tagjainak, a szolgáltatások esetleges támadás miatti kiesése (megbénulása) pedig nemcsak helyi, hanem régiós, de akár globális szintű problémát is okozhat – nem véletlen, hogy ezen rendszerek közül számos rendszer létfontosságú rendszerelemnek minősül[107]. Itt fontos megemlíteni a személyes adatokkal kapcsolatos kockázatokat, mivel az IoT-eszközökön keresztül ezek az adatok kiszivároghatnak. Ilyen eseményt ír le például a Nemzeti Adatvédelmi és Információszabadság Hatóság NAIH/2018/356/3/H (előzmény: NAIH/2017/3979/H)[108] határozata.

A komplex IoT-rendszerek kockázatai jelentős nemzetbiztonsági kockázatot is jelenthetnek, különösen a tömegközlekedés, intelligens utak, kapcsolódó járművek, okos repülőtér, létfontosságú infrastruktúrák esetén, de nem szabad figyelmen kívül hagyni az olyan új rendszereket sem, mint például az állami szinten működtetett Covid19 alkalmazások. A kockázatokat csökkenthetik:

- adminisztratív intézkedések, szabályzatok, protokollok megalkotása, betartása valamint betartatása,[109]
- szervezeti intézkedések (eszköz életciklusának megfelelő biztonsági intézkedések, incidenskezelés, sérülékenységek kezelése, képzés és tudatosság, harmadik felekkel kapcsolatos kockázatok kezelése stb.),
- technikai intézkedések (megbízhatóság és integritásmenedzsment, felhőbiztonság, üzletmenet-folytonosság biztosítása és helyreállítás, gép-gép kommunikáció biztonsága, szoftver/firmware frissítések, hozzáférés menedzsment, protokoll implementációk, anonimizálás, titkosítás, hálózatszegmentálás, figyelemmel kísérés, ellenőrzés és audit, konfiguráció menedzsment stb.).

[105] ENISA: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017. p. 34.

[106] Például okos kórház, okos reptér, közút és vasút, okos tömegközlekedés, okos város stb.

[107] Lásd a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény rendelkezéseit.

[108] Forrás: https://www.naih.hu/files/NAIH-2018-356-H_hatarozat.pdf (Letöltés ideje: 2022. 02. 22.)

[109] security & privacy by design, eszközgazdálkodás, kockázat és fenyegetéskezelés stb.

Otthoni IoT-rendszerek kockázata (IoT Home)[110]

Az IoT-rendszerek kockázatmenedzselése során semmiképpen sem szabad lebecsülni a privát hálózatok[111] jelentőségét, különösen az otthoni hálózatok tükrében. Az otthoni IoT-ökoszisztémák nagy többsége – ellentétben a tudatosan tervezett hálózatokkal – véletlenszerűen beszerzett és egy hálózatba kapcsolt legkülönfélébb IoT eszközök halmaza, amelyek biztonsági kockázata már önálló eszközönként is magas. Főleg, ha azt vesszük figyelembe, hogy ezeknek a hálózati eszközöknek a tulajdonosai/felhasználói a tagjai rendvédelmi dolgozók is lehetnek. A kockázatot növelik az alábbi jellegzetességek:

– a csatlakoztathatóság mindig jelen van az eszközökben;
– az eszköz többféle kommunikációs protokollhoz kapcsolódhat;
– több, egymással összekapcsolt hálózathoz is kapcsolódhat az eszköz az otthonon belül[112] és az otthonon kívül is[113].

Az intelligens otthoni hálózatok jellemzően két csoportba tartozó eszközt tartamaznak:

– az RFC 7228[114] meghatározása szerinti[115] korlátozott eszközök. Ezeknek az eszközöknek a biztonsága korlátozott, viszonylag alacsony is lehet a kapacitásuk miatt;
– nagy kapacitású eszközök, amelyek jellemzően hálózati tápellátással működnek. Ezek az eszközök olyan számítási teljesítménnyel rendelkeznek, amelyeknek köszönhetően fejlett biztonsági funkciókra is képesek lehetnek.

Az „otthoni" eszközök képesek lehetnek távoli szolgáltatásokkal való interakciókra és adatcserére, beleértve a távoli aktiválást, a távoli tárolást vagy tartalomkezelést, az eszközadminisztrációt és az elemzést[116], ezen kívül jellemző lehet rájuk a mobilalkalmazásokkal való interakciók és adatcsere vezérlési/parancsnoki célokra, és az eszközök közötti adatcsere[117].

Az otthoni rendszerek kockázatosságát jelzi az az Egyesült Királyságban benyújtott törvényjavaslat[118], amely az otthonok biztonságát szem előtt tartva három alapvető szabályt tartalmaz:

---

[110] ENISA: Security and Resilience of Smart Home Environments Good Practices and Recommendations; 2015 December

[111] Private Area Network – PAN

[112] Home Area Networks – HAN

[113] Wide Area Networks – WAN

[114] Terminology for Constrained-Node Networks - korlátozott képességű IoT eszközök fogalmainak szaknyelvi gyűjteménye

[115] Internet Engineering Task Force (IETF): Terminology for Constrained-Node Networks, 2014. https://www.rfc-editor.org/rfc/pdfrfc/rfc7228.txt.pdf (Letöltés ideje: 2022. 02. 22.)

[116] IP-tévé, házi robot, mosogatógép, tablet, riasztóközpont, okos játék, okos kutya-macska nyakörv, akvárium hőmérő stb.

[117] Okos telefonnal irányítható redőny, öntöző rendszer avagy a házautomatizálási rendszerek többsége.

[118] Product Security and Telecommunications Infrastructure Bill, https://bills.parliament.uk/bills/3069 (Letöltés ideje: 2022. 02. 22.)

– az eszközökre előre feltöltött, könnyen kitalálható alapértelmezett jelszavakat betiltják, a törvény hatályba lépése után minden termékhez olyan egyedi jelszó szükséges, amelyet nem lehet visszaállítani a gyári alapértelmezettre;
– a fogyasztókkal a készülék megvásárlásakor közölni kell, hogy a készülék minimum mennyi időn belül kapja meg a kulcsfontosságú biztonsági frissítéseket és javító csomagokat. Ha egy termék egyiket sem kapja meg, erről tájékoztatni kell a fogyasztókat;
– a biztonsági kutatást végzőknek nyilvános elérhetőséget kell biztosítani a hibák és hiányosságok jelzésére.

A javaslat szerint az új szabályozás nemcsak a digitális termékek gyártóira fog vonatkozni, hanem azokra a vállalkozásokra is, amelyek olcsó technológiai importtermékeket értékesítenek az Egyesült Királyságban; az előírások megszegése esetén pedig a felügyeleti hatóságnak joga lesz bírságot kiszabni, amelynek mértéke 10 millió fontig, vagy vállalkozás globális forgalmának 4%-áig, illetve folyamatos jogsértés esetén napi 20 ezer fontig terjedhet.

Az Egyesült Államokban a Tapplock-esetben kiderült – szemben a fogyasztói tájékoztatásban ígértekkel –, hogy az okos zárakat (egy hátsó kapu kihasználásával) távoli eléréssel nyitni-zárni lehetett arra jogosulatlanoknak is, illetve sebezhetőségi problémát találtak a felhasználói fiókban tárolt adatokkal kapcsolatban is (felhasználói azonosítók, jelszavak, zárak geolokációs adatai stb.).[119]

Az intelligens otthonokat érintő támadások esetében komplex kockázatokkal kell számolni, melyek jellegzetességei:[120]
– a gyenge védelemmel rendelkező eszközök támadásával a viszonylag kevés ismerettel rendelkező támadók is megpróbálkozhatnak,
– a fizikai támadások jól azonosítható támadásból származnak,
– gyakran olyan eszköz felől történik a támadás, amelyre senki sem számít,[121]
– a nem szándékos, azaz véletlen károkat általában a helytelen bizalmi kapcsolatok eredményezik, és gyakori az emberi hiba is, a lehetséges következmény pedig lehet adatszivárgás, jogosulatlan módosítás vagy akár teljes adatvesztés is,
– az eszközök tulajdonosai – adatvédelmi és adatbiztonsági ismeretek híján – általában nem tudják, mely adataik vannak veszélyben, ezen adatok birtokukból kikerülése nekik milyen károkat okozhat, illetve hogyan előzhetnék meg ezeket a támadásokat (pld. biztonsági frissítések stb.),
– az intelligens otthonban tartózkodók élete is veszélybe kerülhet (pld. intelligens füst- vagy CO_2-érzékelő paramétereinek módosítása),

[119] Federal Trade Commission 2020 Privacy and Data Security Update, 3.o. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf (Letöltés ideje: 2022. 02. 22.)

[120] ENISA: Security and Resilience of Smart Home Environments Good Practices and Recommendations, 2015 december

[121] Akvárium hőmérője, kutya intelligens nyakörve, macskának piros lézerpontot vetítő, 360 fokban látó kamerás kütyü, a gyerekjáték, okos mosogatógép, kamerás kaputelefon, szobabicikli, voice assisstant stb.

– Az intelligens otthonok esetében is jelentős kockázatforrás az, amikor a lecserélt készülékek teljes adattartalmukkal együtt kerülnek a hulladékfeldolgozóba (szeméttelepre, lomtalanítás során a lomok közé), amelynek következtében személyes, gyakran az adatok különleges kategóriájába tartozó személyes adatok szivároghatnak ki.

Speciális[122] IoT-ökoszisztémák

A Covid19-járvány rámutatott az IoT-eszközök alkalmazhatóságának extrém rugalmasságára – a helyzet súlyosbodásával megjelentek a különböző kontaktkutató és -követő alkalmazások, amelyek az okostelefonok hálózatára és azok helymeghatározó adataira építve tették lehetővé a járvány terjedésének nyomon követését, a fertőzöttek mozgását[123]. Az adatvédelem meghatározott szereplői is véleményt nyilvánítottak a témában, így például az Európai Adatvédelmi Testület iránymutatásában[124] leszögezte, a Covid19 elleni küzdelemhez használt adatokat és technológiát inkább az egyének szerepvállalásának növelésére, mintsem ellenőrzésére, megbélyegzésére vagy elnyomására kell felhasználni, és csakis kiegészítő szerepet játszhatnak más közegészségügyi intézkedések hatékonyságának növelése során.

IoT-eszközök adatvédelmi jogi szabályozása

Jogszabályi környezet az Európa Unióban és Magyarországon

Az IoT-eszközök legfontosabb funkciója az adatokhoz kötődik,[125] ezen adatok között pedig számtalan személyes adat, illetve olyan személyes adat van, amely a különleges adatok kategóriájába tartozik. Ezen kívül vannak más típusú adatok is, például környezeti adatok, ezek pedig egyre hangsúlyosabbak lesznek a fenntarthatóság és a klímaváltozás elleni küzdelem szempontjából (pld. ökológiailábnyom-mérés, ESG-keretrendszer,[126] fenntarthatóság-jelentés készítése[127] stb.)

Az IPAR 4.0 okozta robbanásszerű fejlődést az adatvédelmi jogalkotás rohamléptekben próbálja nyomon követni és kezelni az újabbnál újabb kihívásokat. Erre a folyamatra hívja fel a figyelmet az az Európai Gazdasági és Szociális

---

122 adhoc

123 A vírus terjedésének modellezése, a kijárási korlátozások általános hatékonyságának értékelése, kontaktok felkutatása, karantén szabályok betartásának ellenőrzése stb.

124 Európai Adatvédelmi Testület: 04/2020 sz. iránymutatás a Covid19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használatáról, elfogadás időpontja: 2020. április 21.

125 Gyűjtés, tárolás, feldolgozás, továbbítás stb.

126 ESG (Environment, Social, Governance) - olyan keretrendszer, amelynek az a célja, hogy a pénz- és tőkepiaci szereplők a fenntarthatóság szempontjából objektíven ítélhessék meg a gazdálkodó szervezetek tevékenységét; három fő területe a környezeti hatások vizsgálata, a társadalmi kérdések kezelése és a vezetői döntéshozatal folyamata.

127 Például Magyar Nemzeti Bank Fenntarthatósági jelentés 2021. https://www.mnb.hu/kiadvanyok/jelentesek/fenntarthatosagi-jelentes/fenntarthatosagi-jelentes-2021 (Letöltés ideje: 2022. 02. 22.)

Bizottság[128] véleménye, amelynek tárgya a bizalom, a magánélet tiszteletben tartása, és biztonság a fogyasztók és a vállalkozások számára a dolgok internetén,[129] emellett az IoT-világban egyre gyakrabban használt mesterséges intelligenciával kapcsolatban is folyik speciálisan erre a területre vonatkozó rendelet előkészítése.

Az IoT uniós adatvédelmi szabályozása jelenleg – alapvetően, de nem kizárólag – három pilléren nyugszik:

– a GDPR,
– a bűnügyi adatvédelmi irányelv[130] (implementációja a magyar jogban az Infotv.), illetve
– az elektronikus hírközlési adatvédelmi irányelv[131] („ePrivacy irányelv"), amely utóbbi rendelkezései a magyar jogban az elektronikus hírközlésről szóló 2003. évi C. törvényben („Eht.") találhatóak meg.

Az uniós jogi szabályozásban az IoT-rendszerekkel kapcsolatban újabb jelentős lépések várhatóak, például a mesterséges intelligencia használatával, a kapcsolt rendszerekkel, a digitális piaccal és digitális szolgáltatásokkal kapcsolatos rendeletek elfogadása és hatályba lépése.

Az általános adatvédelmi rendelet

A GDPR 2. cikk (1) bekezdése alapján az általános adatvédelmi rendeletet kell alkalmazni *„a személyes adatok részben vagy teljes egészében automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni."* A kivételeket ugyanezen cikk (2) bekezdése sorolja fel, miszerint a rendelet nem alkalmazandó a személyes adatok kezelésére, ha azt:
„a) az uniós jog hatályán kívül eső tevékenységek során végzik;

[128] Az Európai Gazdasági és Szociális Bizottság az Európai Unió konzultatív szerve, (329) taggal - EGSZB

[129] Az Európai Gazdasági és Szociális Bizottság véleménye – Bizalom, a magánélet tiszteletben tartása és biztonság a fogyasztók és a vállalkozások számára a dolgok internetén (2018/C 440/02), https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018IE1038&from=DA (Letöltés ideje: 2022. 02. 22.)

[130] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L0680&from=hu#d1e893-89-1 (Letöltés ideje: 2022. 02. 22.)

[131] a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (elektronikus hírközlési adatvédelmi irányelv), https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU (Letöltés ideje: 2022. 02. 22.)

b) a tagállamok az EUSZ V. címe 2. fejezetének hatálya alá tartozó tevékenységek során végzik;[132]

c) természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik;[133]

d) az illetékes hatóságok bűncselekmények megelőzése, nyomozása, felderítése, vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzik, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését."

Nem tartozik továbbá a GDPR hatálya alá az adatkezelés, ha

a) uniós intézmények, szervek, hivatalok és ügynökségek végzik az (EU) 2018/1725 rendelet[134] szerint,[135]

b) tagállamok nemzetbiztonsági céllal végzik. Ezek az adatkezelések teljes mértékben kívül esnek az uniós jogon, sőt még az Alapjogi Charta hatályán is, azonban az ilyen adatkezelésekre is vonatkozik az Emberi Jogok Európai Egyezménye és az Emberi Jogok Európai Bíróságának joghatósága alá tartoznak[136]).

A GDPR határozza meg az adatvédelmi jog alapfogalmait (pld. személyes adat, adatkezelő, adatkezelés, harmadik ország, adatvédelmi incidens stb.), illetve lefekteti az adatkezelés konstrukcióinak követelményeit (pld. adatfeldolgozás, közös adatkezelés, adattovábbítások stb.), az érintetti jogokat valamint a felügyeleti hatóságok és az Európai Adatvédelmi Testület szerepét.

---

[132] Közös kül- és biztonságpolitika

[133] Úgynevezett. „háztartási adatkezelés"

[134] Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R1725&from=HU (Letöltés ideje: 2022. 02. 22.)

[135] (EU) 2018/1725 rendelet 2. cikk (1) bekezdése alapján ezt a rendeletet kell alkalmazni a személyes adatok valamennyi uniós intézmény és szerv általi kezelésére. A rendelet (5) preambulumbekezdése alapján a személyes adatok védelmének az Unión belüli egységes megközelítése és a személyes adatok Unión belüli szabad áramlása érdekében a lehető legnagyobb mértékben összhangba kell hozni az uniós intézményekre, szervekre, hivatalokra és ügynökségekre vonatkozó adatvédelmi szabályokat a tagállamokban a közszféra számára elfogadott adatvédelmi szabályokkal. Amennyiben a (EU) 2018/1725 rendelet rendelkezései ugyanazon elveket követik, mint az (EU) 2016/679 rendelet rendelkezései, ezen két rendelet rendelkezéseit az Európai Unió Bírósága (a továbbiakban: a Bíróság) ítélkezési gyakorlata szerint egységesen kell értelmezni, különösen mivel a (EU) 2018/1725 rendelet struktúrája az (EU) 2016/679 rendelet struktúrájával egyenértékűnek tekintendő.

[136] European Court of Human Rights, Research Division: National security And European case-law, 2013. https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf (Letöltés ideje: 2022. 02. 22.)

ePrivacy irányelv

Az elektronikus hírközlési adatvédelmi irányelv 1. cikkének (2) bekezdése kimondja, hogy az irányelvnek a rendelkezései pontosítják és kiegészítik a GDPR rendelkezéseit, illetve rendelkezik a jogi személyiséggel rendelkező előfizetők jogos érdekeinek védelméről is.

Az irányelv első bekezdése egyértelműsíti a két jogforrás kapcsolatát, e szerint az elektronikus hírközlési ágazatban a GDPR alkalmazandó az alapvető jogok és szabadságok védelmével kapcsolatos azon területekre, amelyet az irányelv rendelkezései nem kifejezetten szabályoznak, beleértve az adatkezelők kötelezettségeit és az egyének jogait, illetve a GDPR alkalmazandó a nem nyilvános hírközlési szolgáltatásokra.

Az irányelv ugyan alkalmazandó az IoT-rendszerekre is, de – már csak elfogadásának időpontjából adódóan is – a megfelelősége nem minden téren felel meg a modern kor elvárásainak. Az irányelvet a közeljövőben várhatóan felváltja majd az ePrivacy rendelet, amely – a GDPR-hoz hasonlóan – közvetlenül alkalmazandó uniós rendelet lesz, és amely már az IoT rendszerek sajátosságaira figyelemmel készül. A tervezet szövegét az EU Tanácsa 2021 februárjában elfogadta, ezt követően az Európai Bizottság, az Európai Parlament és az EU Tanácsa tárgyal az ePrivacy rendelet véglegesítéséről.

Az ePrivacy rendelet az M2M-, VoIP-[137] és IoT-szolgáltatásokra is alkalmazandó, mivel azok az Európai Elektronikus Hírközlési Kódex (EECC) alapján elektronikus hírközlési szolgáltatásnak minősülnek, feltéve, hogy a jelek továbbítása nyilvánosan elérhető elektronikus hírközlési szolgáltatáson vagy hálózaton keresztül történik, és a kommunikáció a kommunikáció feladója és az általa meghatározott korlátozott számú végfelhasználó között zajlik. A rendelet hatálya nem terjed ki a szervezetek intranetjén keresztül történő belső kommunikációra, az olyan kommunikációra, amely ügyfélszolgálati csatornán keresztül valósul meg, és ahol az ügyfelek csak az érintett szervezettel kommunikálhatnak, illetve az olyan csatornákra, amelyek nyitottak mindenki számára (pld. online játékok).[138]

Hazai szabályozás

A hazai IoT-szabályozás főbb pillérei adatvédelmi téren a

- GDPR, illetve a GDPR-t kiegészítő Infotv.,
- a bűnügyi, honvédelmi és nemzetbiztonsági célú adatkezelések esetében az Infotv.,
- az Eht. (ePrivacy irányelv implementálása terén), illetve
- az IoT-rendszerek egyes területeit külön ágazati jogszabályok is érinthetik.[139]

---

[137] Voice over IP

[138] Forrás: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf (Letöltés ideje: 2022. 02. 22.)

[139] Például az MNHH rendeletek vagy a villamos energiáról szóló 2007. évi LXXXVI. törvény egyes rendelkezéseinek végrehajtásáról szóló 273/2007. (X. 19.) Korm. rendelet az okosmérők esetében.

Jogértelmezés az Európa Unióban

A jogi szabályozás az Unióban számtalan kihívással szembesül, ezek jórésze szorosan kapcsolódik globális eseményekhez, illetve társadalmi trendekhez, például:

- az internetes kereskedelemnek köszönhetően ma már bárki bármikor könnyedén, megfizethető összegért képes beszerezni, és üzembe tud állítani olyan IoT-eszközt, amelynek használata uniós és/vagy tagállami jogba ütközhet. Számtalan (távol-keleti) internetes áruház értékesít okos szemüveget beépített kamerával és internetes böngészővel[140], miközben viselése – ritka kivételtől eltekintve – sérti az Alapjogi Chartát, a forgalmazás tiltása pedig leírva szépen mutat, de a gyakorlatban számtalan nehézségbe ütközik;
- Az adatkezelők nem célhoz kötött adatkezelése, például a járványhelyzetre készült követő, illetve kontaktazonosító applikációk adatainak reklámozási célú felhasználása, illetve a kiemelten fontos szenzitív adatok (például geolokációs adatok) különféle marketing és egyéb célú felhasználása;
- a személyes adatok korlátlan adása-vétele, különös tekintettel az érintettek tudta nélkül különféle leányvállalatokon és adatbrókereken keresztül átadása, az adatok vegyítése, adatbázisok összekötése, új adatok előállítása, az érintettek számtalan módon történő profilozása;
- A kiberbűnözés súlypontjainak eltolódása a zsarolóvírusok és adathalászat irányába, amelyek nemcsak szervezetekre, hanem magánszemélyekre is egyre növekvő kockázatot jelentenek.

A dinamikus technikai és társadalmi fejlődést a jogalkotás csak jelentős lépéshátránnyal tudja követni, így a frissen felmerülő problémák esetében elsődlegesen a hatályban lévő uniós jogszabályokkal kapcsolatos hivatalos jogértelmezések nyújthatnak segítséget.

Az uniós adatvédelmi irányelvek értelmezésével kapcsolatban a GDPR kötelező alkalmazásáig a 29. cikk szerinti Adatvédelmi Munkacsoport adott ki iránymutatásokat, ezt követően a GDPR alapján létrejött Európai Adatvédelmi Testület (EDPB[141]) segíti a jogértelmezést. A már említett IoT-vélemény[142] mellett számtalan olyan dokumentum készült, amely több-kevesebb eligazítást ad egy-egy terület problémáiról, így például az intelligens közlekedési rendszerekkel, a kapcsolódó járművekkel, az okos mérőkkel, vagy éppen a Virtual Voice Assisstant-tel kapcsolatban. Ilyen típusú eszközök a különféle beszerzések során bekerülhetnek honvédelmi környezetbe is (pld. szolgálati gépjárművek, drónok stb.), a vonatkozó véleményekben és iránymutatásokban foglaltak felhasználásával pedig jelentősen csökkenthetők az adatvédelmi kockázatok.

---

[140] Ezen a téren változás várható a kínai tiltás miatt, lásd ANI: China launches fresh crackdown on spy cameras in a bid to tighten digital privacy laws, 2021. június 15., https://in.news.yahoo.com/china-launches-fresh-crackdown-spy-170657587.html (Letöltés ideje: 2022. 02. 22.)

[141] European Data Protection Board

[142] 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16.

Az IoT-rendszerek adatbiztonsága téren – különös tekintettel a kiberbiztonságra – az ENISA[143] bocsátott ki számtalan dokumentumot, amelyek részletes tanácsokkal látják el az információbiztonsággal foglalkozó szakembereket. Ezen kívül az ENISA évente közreadja a kiberfenyegetések trendjeiről szóló tájékoztatóit, a 2021-es kiadvány[144] egyik hangsúlyos pontja pedig az IoT-rendszerekkel kapcsolatos új típusú támadások.

A bűnügyi adatvédelmi irányelv által lefedett területeken is ad ki iránymutatásokat az EDPB, a jogértelmezés és jogegységesítés utolsó bástyái pedig a bíróságok, különös tekintettel az Európa Unió Bíróságára.

IoT az Európa Unión kívül

Míg az Európa Unió területén viszonylag egységes joggyakorlattal találkozunk, az Unió határain túl komplex helyzettel állunk szemben. Ez azonban nem a használt IoT-rendszerek eltéréseiből fakad, hanem abból, hogy magával az adatvédelemre[145] irányadó jogi környezettel kapcsolatban vannak országonként eltérő gyakorlatok. Az Amerikai Egyesült Államokban például teljesen elfogadott az, hogy szomszédfigyelő rendszer keretében az egy környéken lakók egy rendszerbe kötik be az ingatlanjuk előtti közterület is megfigyelő video-kaputelefonjukat, illetve egyéb eszközeiket[146], miközben az ilyen típusú közterületmegfigyelés egy GDPR hatálya alá tartozó országban nagy valószínűséggel jogszerűtlen lenne. Hasonló aggályok merülhetnek fel például a gépjárművek fedélzeti kamerájával kapcsolatban is, hiszen a járművel együtt mozgó IoT-kamerák honvédelmi/nemzetbiztonsági objektumot vagy területet is megfigyelhetnek.

Ezeket a megoldásokat és jogszabályi különbségeket minden, több régiót érintő IoT-ökoszisztéma esetén fel kell térképezni, és az eltérő joghatóságokból[147] fakadó kockázatokat is figyelembe kell venni a rendszerek kiépítésénél, összehangolásánál és üzemeltetésénél.

A kockázatcsökkentés lehetősége

A 29. cikk szerinti Adatvédelmi Munkacsoport korábban említett véleményében[148] – többek között – szorgalmazza, hogy:

---

[143] The European Union Agency for Cybersecurity; https://www.enisa.europa.eu/about-enisa (Letöltés ideje: 2022. 02. 22.)

[144] ENISA THREAT LANDSCAPE 2021; 2021. október

[145] Információs önrendelkezési joggal

[146] CERICOLA, Rachel: Ring Neighbors Is the Best and Worst Neighborhood Watch App; June 3, 2021, https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/ (Letöltés ideje: 2022. 02. 22.)

[147] Például adatkezelések felügyeleti hatósági vagy bírósági úton betiltása, büntetések, kártérítés fizetési kötelezettség stb.

[148] 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16.

- mielőtt bármilyen új alkalmazás bevezetése történik az IoT-rendszerben, az adatkezelő folytasson le adatvédelmi hatásvizsgálatot (DPIA[149]), felmérve az adatkezelés kockázatait, valamint a felhasználókra gyakorolt hatását. Korábban az RFID tekintetében[150] a Munkacsoport konkrét ajánlásokat is megfogalmazott az adatvédelmi hatásvizsgálatokkal kapcsolatban, a GDPR bevezetése óta pedig nemcsak ajánlás, hanem – a jogszabály által meghatározott esetekben – alapkövetelmény is adatvédelmi hatásvizsgálat lefolytatása,[151] a megfelelést pedig a NAIH által is ajánlott szoftver alkalmazása segítheti;[152]
- Az IoT-eszközök esetében biztosítani kell az adatok helyben olvashatóságát és szerkeszthetőségét (felhasználóbarát felületen) még az adattovábbítás előtt, illetve az adatok hordozhatóságát is;
- A gyártóknak és alkalmazásfejlesztőknek biztosítani kell a frissítéseket (sebezhetőségi problémák megoldását), illetve a felhasználókat tájékoztatni kell arról is, ha megszűnik a támogatás;
- Az IoT-eszközök esetében lehetővé kell tenni a többfelhasználós megoldást, és azt, hogy a felhasználók ne ismerhessék meg egymás tevékenységét (pld. intelligens otthonok esetében több személy is használhatja ugyanazt az eszközt). Ez különösen gondot jelenthet olyan esetekben, mint amikor például egy internetszolgáltató családi előfizetés keretében több eszközről is gyűjt adatokat, azokat vegyíti, és marketing célra felhasználja, miközben ezek az adatok a család több tagjától is származhatnak (pld. böngészési, vásárlási adatok);
- Az IoT-eszközök által a közösségi platformokon közzétett információk alapértelmezés szerint még a közzététel előtt szerkeszthetők legyenek, valamint ne váljanak szabadon nyilvánossá, és a kereső motorok ne indexelhessék azokat.

A 29. cikk szerinti Adatvédelmi Munkacsoport – a már említett dokumentumon kívül – számos iránymutatásában és véleményében írt az intelligens eszközökről, és utódja, az EDPB folytatja a technikai fejlődés adatvédelmi jogi vetületének magyarázatát és értelmezését olyan területekre koncentrálva, mint például:

– az elektronikus kommunikáció hírszerzési és nemzetbiztonsági célú megfigyelése,[153]
– az anonimizálási technikák,[154]

---

[149] Data Protection Impact Assessment

[150] 29. cikk szerinti Adatvédelmi Munkacsoport 9/2011. számú vélemény a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló felülvizsgált ágazati javaslatról (WP180) melléklete: Privacy and Data Protection Impact Assessment Framework for RFID Applications 2011. január 12. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf (Letöltés ideje: 2022. 02. 22.)

[151] 29. cikk szerinti Adatvédelmi Munkacsoport Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e (WP 248 rev.01), az elfogadás időpontja: 2017. április 4; a legutóbbi felülvizsgálat és elfogadás időpontja: 2017. október 4. https://www.naih.hu/files/WP248_rev01_hu.pdf

[152] https://naih.hu/hatasvizsgalati-szoftver (Letöltés ideje: 2022. 02. 22.)

[153] 29. cikk szerinti Adatvédelmi Munkacsoport: 4/2014. sz. vélemény az elektronikus kommunikáció hírszerzési és nemzetbiztonsági célú megfigyeléséről (WP215)

[154] 29. cikk szerinti Adatvédelmi Munkacsoport: 05/2014. számú vélemény az anonimizálási technikákról (WP216)

– drónok,[155]
– a munkahelyi adatkezelés (az információs és kommunikációs technológiák munkahelyi használata is),[156]
– az automatizált döntéshozatal és a profilalkotás,[157]
– kooperatív intelligens közlekedési rendszerek (C-ITS),[158]
– beépített és alapértelmezett adatvédelem,[159]
– személyes adatok videoeszközökkel történő kezelése,[160]
– kapcsolódó járművek,[161]
– Virtual Voice Assistants.[162]

Ezen iránymutatásokban és véleményekben foglalt jó gyakorlatok alkalmazása jelentősen csökkentheti az adatkezelők kockázatát az IoT-rendszerekkel kapcsolatban.

A járványhelyzet tekintettel az EDPB több iránymutatást is kiadott (például a Covid19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használata,[163] illetve a kontaktkövető alkalmazások interoperabilitásának adatvédelmi hatásai[164]), tekintettel az új technológiák alkalmazására és alkalmazhatóságára.

„Az adatvédelmi szabályok (például a GDPR) nem akadályozhatják a koronavírus világjárvány elleni küzdelemben hozott intézkedéseket. A fertőző betegségek elleni küzdelem minden nemzet közös célkitűzése, ezért azt a lehető legjobb módon kell támogatni. Az emberiség érdeke, hogy megfékezze a betegségek terjedését, és modern technikákat alkalmazzon a világ nagy részeit érintő csapások elleni küzdelemben. Ennek ellenére az EDPB hangsúlyozni kívánja, hogy ***még ezekben az extrém időkben is az adatkezelőnek és az adatfeldolgozónak biztosítania kell az érintettek személyes adatainak védelmét****. Ezért számos szempontot figyelembe kell venni a*

[155] Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones (WP231)

[156] 29. cikk szerinti Adatvédelmi Munkacsoport: 2/2017. számú vélemény a munkahelyi adatkezelésről (WP249)

[157] 29. cikk szerinti Adatvédelmi Munkacsoport: Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához, elfogadás időpontja: 2017. október 3. A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6. (WP251rev.01)

[158] 29. cikk szerinti Adatvédelmi Munkacsoport: 03/2017. számú vélemény a személyes adatok kooperatív intelligens közlekedési rendszerek (C-ITS) keretében történő kezeléséről (WP252)

[159] EDPB 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat, elfogadás időpontja: 2020. október 20.

[160] EDPB 3/2019. számú iránymutatás a személyes adatok videoeszközökkel történő kezeléséről, 2.0 változat, elfogadás időpontja: 2020. január 29.

[161] EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, version 2.0, adopted on 2021. március 29.

[162] EDPB Guidelines 02/2021 on Virtual Voice Assistants, version 1.0, adopted on 2021. március 9.

[163] EDPB 04/2020 sz. iránymutatás a COVID19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használatáról, elfogadás időpontja: 2020. április 21.

[164] EDPB Nyilatkozat a kontaktkövető alkalmazások interoperabilitásának adatvédelmi hatásáról, elfogadás időpontja: 2020. június 16.

személyesadatok jogszerű kezelésének garantálása érdekében, és minden esetben emlékeztetni kell arra, hogy az ebben az összefüggésben hozott intézkedéseknek tiszteletben kell tartaniuk az általános elveket, azokkal nem lehetnek ellentétesek. A vészhelyzet olyan jogi feltétel, amely legitimálhatja az egyének szabadságának korlátozását, feltéve, hogy ezek a korlátozások arányosak és csak a vészhelyzet idejére korlátozódnak.
(...)
A távközlési adatok – például a helymeghatározási adatok – kezelése során tiszteletben kell tartani. Az elektronikus hírközlési adatvédelmi irányelvet végrehajtó nemzeti jogszabályokat. Elvben a helymeghatározási adatokat csak az adatkezelő kezelheti anonim módon vagy a magánszemélyek hozzájárulásával. Azonban az elektronikus hírközlési adatvédelmi irányelv 15. cikke lehetővé teszi a tagállamok számára, hogy jogalkotási intézkedéseket vezessenek be a közbiztonság védelme érdekében. Az ilyen kivételes szabályozás csak akkor lehetséges, ha szükséges, megfelelő és arányos intézkedést jelent egydemokratikus társadalomban. Ezeknek az intézkedéseknek összhangban kell lenniük az Alapjogi Chartával és Az emberi jogok és alapvető szabadságok védelméről szóló európai egyezménnyel. Ezenkívül az Európai Bíróság és az Emberi Jogok Európai Bírósága igazságügyi ellenőrzése alá tartozik. Vészhelyzet esetén azt szigorúan a kezelt vészhelyzet időtartamára kell korlátozni. "[165]

A kockázatok csökkentésében segítséget nyújthatnak az ENISA kiberbiztonsággal kapcsolatos tájékoztatásai. Az ENISA rangsorolása alapján[166] 2020. április és 2021 júliusa közötti időszak kiberfenyegetései:

- zsaroló vírus,
- rosszindulatú kód,
- Cryptojacking,
- e-mailhez kapcsolódó fenyegetések,
- adatokhoz kapcsolódó fenyegetések,[167]
- rendelkezésre állás és az integritás elleni fenyegetések,[168]
- megtévesztés és félretájékoztatás,[169]
- nem rosszindulatú támadás,[170]
- beszállítói lánchoz kötődő támadások.[171]

[165] AZ EDPB Nyilatkozata a személyes adatok kezeléséről a COVID-19 járvány kitörésével összefüggésben, elfogadva 2020. március 19-én, pp. 1-2. https://naih.hu/files/edpb-covid-19-nyilatkozat-naih.pdf (Letöltés ideje: 2022. 02. 22.)
[166] ENISA Threat Landscape 2021; 2021. október
[167] Threats against data
[168] Threats against availability and integrity
[169] Disinformation – misinformation
[170] Non-malicious threats
[171] Supply-chain attacks

Az ENISA szerint a legfontosabb tendenciák[172] nagymértékben befolyásolhatják egy-egy szervezet kiberbiztonsággal kapcsolatos stratégiáját:

- a zsarolóvírusok elsődleges fenyegetéssé léptek elő (2019. január és 2020. április közötti időszakban a TOP15 fenyegetés közül „még csak" a 13. helyen szerepelnek ki[173]),
- a kiberbűnözőket egyre inkább motiválja az anyagi haszonszerzés,
- a cryptojacking támadások száma 2021 első negyedévében rekordmagasságot ért el (az előző évi TOP15-ben a 15. volt),
- a Covid19 még mindig a domináns csali az e-mailes támadásokban és megugrott az egészségügyi ágazathoz kapcsolódó támadások száma,
- a hagyományos DDoS[174]-támadások célzottabbá és tartósabbá váltak. 2021-ben az IoT-rendszerek támadása a DDoS-támadások új hullámát eredményezte,
- a Covid19 az emberi hibák és a rendszerhibák multiplikátorává vált,[175] ezekre vezethető vissza a nem rosszindulatú incidensek számának megugrása,
- az ENISA külön dokumentumban[176] foglalkozott a beszállító rendszerekkel kapcsolatos támadásokkal mind újszerűségük, mind a volumenük, mind pedig a nemzetbiztonsági kockázatuk miatt.

A Kroll az ENISA illetékeseihez hasonlóan értékeli az adatvédelmi incidensek számának 2020. évi növekedése mögötti tényezőket[177]:

- a távmunkára való áttérés miatt a munkavállalók sokkal kiszolgáltatottabbak a kiberbűnözéssel szemben,
- a zsarolóvírusok átalakultak komplex zsarolási rendszerekké,
- az ellátási láncokat ért támadások száma jelentősen növekedett,
- az építőipar volt a legsebezhetőbb IoT-specifikus fenyegetésekkel szemben.

[172] ENISA Threat Landscape 2021; 2021 október
[173] ENISA Threat Landscape – List of Top 15 Threats from January 2019 to April 2020
[174] Distributed Denial of Service
[175] Erőltetett, rohamtempójú digitális transzformáció, otthoni munkvégzés stb.
[176] ENISA Threat Landscape for Supply Chain Attacks, 2021. július 29; www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (Letöltés ideje: 2022. 02. 22.)
[177] Kroll: 2021 Data Breach Outlook; https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021 (Letöltés ideje: 2022. 02. 22.)

Az IoT-szektor jellemző fenyegetései

Az ENISA az alábbi fenyegetéstípusokra hívta fel a figyelmet[178]:

Területek	*Fenyegetést jelentő események*
humánerőforrás	Belső fenyegetés, csapatmunkával kapcsolatos problémák, belső korlátok, hacktivista tevékenység, támogatási szolgáltatások elvesztése, közműkiesés, hálózatkiesés, nem szándékos módosítások, szabotázs, jogszabályok és előírások megsértése, szerződéses követelmények nem teljesítése (pld. szoftverkarbantartás), szoftverhibák, manipuláció,[179] személyazonosság-lopás.[180]
szoftvertervezés	Belső fenyegetés, hacktivizmus, nem szándékos módosítások, szabotázs, az eszközök és rendszerek hibás használata, szoftverfejlesztési életciklus (SDLC[181]) folyamatainak hibái, harmadik fél hibái, a szerződéses követelmények nem teljesítése (pld. szoftverkarbantartás), szoftverhibák, információvesztés/szivárgás.
szoftverfejlesztés	Belső fenyegetés, hacktivista tevékenység, támogató szolgáltatások elvesztése, nem szándékos módosítások, eszközök és rendszerek hibás használata, szabotázs, vandalizmus és lopás, szoftversebezhetőségek, SDLC-folyamatok hibái, karbantartási hibák, jogosultsággal való visszaélés, szoftverhibák, SDLC-infrastruktúra manipulálása, információvesztés/szivárgás.
szoftvertelepítés	Bennfentes fenyegetés, hacktivista tevékenység, támogató szolgáltatások elvesztése, nem szándékos módosítások, hibás használat vagy adminisztráció, eszközök és rendszerek hibás kezelése, szabotázs, vandalizmus és lopás, szoftversebezhetőségek, SDLC-folyamatok hibái, harmadik fél hibái, jogosultsággal való visszaélés, szoftverhibák, SDLC-infrastruktúra manipulálása, szolgáltatásmegtagadás, információ manipulációja, nyilvánosságra hozatal, az információk elvesztése/szivárgása.

[178] ENISA Threat Landscape: Sectoral/Thematic Threat Analysis From January 2019 to April 2020; p. 10. https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis (Letöltés ideje: 2022. 02. 22.)
[179] social engineering
[180] identity theft
[181] Systems development life cycle

adatok	Bennfentes fenyegetés, hacktivizmus, támogató szolgáltatások elvesztése, nem szándékos módosítások, a rendszerek és eszközök hibás használata vagy adminisztrációja, szabotázs, vandalizmus és lopás, Szoftverek sebezhetőségei, SDLC-folyamatok hibái, harmadik fél hibái, jogosultsággal való visszaélés, szoftverhibák, az SDLC-infrastruktúra manipulálása, szolgáltatásmegtagadás, információmanipuláció, nyilvánosságra hozatal, információvesztés/szivárgás.
karbantartás	Bennfentes fenyegetés, hacktivizmus, közműkimaradás, hálózati kiesés, nem szándékos módosítások, az eszközök és rendszerek hibás használata, harmadik fél által okozott kár, szabotázs, vandalizmus és lopás, fizikai hozzáféréssel járó támadások, kényszerített hozzáférés, szerződéses követelmények, szoftversebezhetőségek, SDLC-folyamatok hibái, harmadik fél hibái, szerződéses követelmények be nem tartása (pld. szoftverkarbantartás), karbantartás-mulasztások, jogosultsággal való visszaélés, szoftverhibák, SDLC-infrastruktúra manipulálása, szolgáltatásmegtagadás, információmanipuláció, nyilvánosságra hozatal, az információk elvesztése/szivárgása.
szoftverek	Bennfentes fenyegetés, hacktivizmus, támogató szolgáltatások elvesztése, nem szándékos módosítások, az eszközök és rendszerek hibás használata, harmadik fél által okozott károk, szabotázs, vandalizmus és lopás, fizikai támadások, kényszerített hozzáférés, szerződéses követelmények, szoftversebezhetőségek, SDLC folyamatok hibái, harmadik fél hibái, szerződéses követelmények nem teljesítése (pld. szoftverkarbantartás), karbantartási hibák, jogosultsággal való visszaélés, szoftverhibák, SDLC-infrastruktúra manipulálása, szolgáltatásmegtagadás, információmanipuláció, nyilvánosságra hozatal, információvesztés/szivárgás.

Technikai-társadalmi változások

Ahogy a korábbi ipari forradalmak, a negyedik ipari forradalom is komoly társadalmi változásokat és olyan mozgalmakat eredményezhet, amelyeket a jogalkotóknak akár uniós, akár tagállami szinten kezelniük kell, és olyan területekre is figyelemmel kell lenniük, mint a nanotechnológia, az additív gyártástechnológia, a mesterséges intelligencia, a gépi tanulás, a blokklánc-technológia, a digitális transzformáció, a virtualizáció, illetve ezek viszonya a felhasználókhoz.

A digitális fejlesztések olyan folyamatokat indíthattak el, amelyeket eddig csak a tudományos-fantasztikus irodalomból és filmekből ismertünk. A technika alkalmazóinak és az alkalmazók felügyeletére kijelölt szervezeteknek önmérsékletre

van szükségük ahhoz, hogy a XXI. század modern demokratikus országai ne váljanak olyan világgá, ahol a megfigyelő rendszerek alkalmazásának elkerülésére lehetőség sincsen.

A totális megfigyelés lehetősége már megvan, és a „felügyeleti kapitalizmus" elmélete[182] pedig megjelent nemcsak a tudományos életben, hanem a közbeszédben is. A polgárok a saját bőrükön tapasztalják meg az új technológiák „vadhajtásait", például amikor mosolyogva kell menniük dolgozni, mert különben az érzelemdetektáló kamera nem engedi be őket a munkahelyükre,[183] vagy az MS Office365 követi minden lépésüket, és profilozza őket, majd ezeket az információkat továbbadja a feletteseiknek.[184] Azonban nemcsak a természetes személyeket figyelhetik meg az állami szervek és a privátcégek, hanem a köznapi embereket és a nagyvállalatokat is, a piac szereplőinek pedig fel kell készülniük egy újfajta fogyasztó megjelenésére – olyanéra, aki akár a technika vívmányait (köztük az IoT-eszközöket) is hajlandó igénybe venni azért, hogy érvényesítse (vagy legalábbis megpróbálja érvényesíteni) fogyasztói jogait.[185]

Mesterséges intelligencia (AI[186])

Az utóbbi években szállóigévé vált a mondás, *„az adat az új olaj"*, a piaci szereplők pedig igyekeznek felkészülni arra a kihívásra, ami elé az elkövetkező évtized állítja őket – a Big4 egyike, a PWC például 12 milliárd dolláros befektetéssel, százezer fővel kívánja bővíteni a munkavállalói körét 2026-ra (284 ezer főről 384 ezer főre) olyan területeken, mint a mesterséges intelligencia és a kiberbiztonság.[187]

A tapasztalt tendenciákra figyelemmel számos ország, köztük Magyarország is elkészítette a mesterséges intelligenciára vonatkozó nemzeti stratégiáját, amely a kiemelt kutatás-fejlesztési célok között szerepelteti az IoT-rendszereket is.[188]
„Gépi tanuláson alapuló intelligens gyártás, logisztika, IoT megoldások fejlesztése

---

[182] ZUBOFF i. m.

[183] VINCENT, James: Canon put AI cameras in its Chinese offices that only let smiling workers inside; The Verge, Jun 17, 2021; https://www.theverge.com/2021/6/17/22538160/ai-camera-smile-recognition-office-workers-china-canon (Letöltés ideje: 2022. 02. 22.)

[184] HERN Alex: Microsoft productivity score feature criticised as workplace surveillance; The Guardian, 26 Nov 2020 https://www.theguardian.com/technology/2020/nov/26/microsoft-productivity-score-feature-criticised-workplace-surveillance (Letöltés ideje: 2022. 02. 22.)

[185] FLANCHER Balázs: Egy magyar twitterező nyomkövetőt tett egy Kaliforniából feladott csomagba, találják ki, mennyi idő alatt jutott el a magyarországi címzetthez; Telex, 2018. június 18. https://telex.hu/zacc/2021/06/18/csomag-airtag-magyar-posta-egyesult-allamok-magyarorszag (Letöltés ideje: 2022. 02. 22.)

[186] artificial intelligence

[187] MAUER, Mark: PwC to Spend $12 Billion on Hiring, Expanding Expertise in AI, Cybersecurity; The Wall Street Journal, June 15, 2021. https://www-wsj-com.cdn.ampproject.org/c/s/www.wsj.com/amp/articles/pwc-to-spend-12-billion-on-hiring-expanding-expertise-in-ai-cybersecurity-11623758400 (Letöltés ideje: 2022. 02. 22.)

[188] Magyarország Mesterséges Intelligencia Stratégiája 2020-2030; 2020. május, p. 26. https://ai-hungary.com/api/v1/companies/15/files/137203/view (Letöltés ideje: 2022. 02. 22.)

A hálózatba kötött gépek és az IoT (Internet of Things, vagyis a dolgok internetje) terjedése miatt exponenciálisan növekvő mennyiségű adat áll rendelkezésre különleges zajtípusokkal és a berendezésektől függő egyedi adatformátummal. A gépi tanulási módszerek lehetővé teszik szabályok, függvények, döntések automatikus, emberi beavatkozás vagy segítség nélküli megtanulását. Pontosabb, megbízhatóbb döntések érdekében nagymennyiségű adat erőforrás-igényes elemzése, összetett optimalizációs és numerikus eljárások tervezése és végrehajtása szükséges. Feladat egy gépi tanuló eljárást tartalmazó rendszer robusztusságának vizsgálata, azaz annak vizsgálata, egy új tanítópont figyelembevétele elrontja-e a rendszer tulajdonságait. Céljaink között szerepel összetett rendszerek irányítása gépi tanuló algoritmussal (model predictive control – MPC), az optimális beavatkozó jel megtanítása, az irányított rendszerre stabilitási garanciák biztosítása."

A Stratégia alapján a meglévő folyamatok esetében kiemelt szakterületek középtávon:
„MI használat 6G hálózatokban, gyártásban; értékesítés utáni termékkövetés, MI alapú adatfeldolgozás, szerviz igények becslése és jelzése; drón menedzsment ipari területen (mintagyár, mintaterület); kritikus gép-gép (M2M) kommunikáció, nagy számú IoT-eszköz és privát kommunikációs eszközök működésének automatizált menedzsmentje ipari területen (minta terület); beszállítói láncok, termékek nyomonkövetése; gyártási logisztika optimalizálása; gyártási energiagazdálkodás optimalizálása; gyártási kiberbiztonság."

A mesterséges intelligenciával kapcsolatos fejlesztések kiterjednek az IoT-ökoszisztémára is, újabb és újabb kihívások elé állítva a biztonsági szakembereket.

Az elgondolás alapján legfőképpen az alábbi területek érintettek:

- személyek azonosítása és profilozása;
- anomizálás és újraazonosítás;
- titkosítás és titkosítás visszafejtése;
- kibertámadások megtervezése és végrehajtása, illetve kibertámadásra utaló jelek figyelése, támadási minták azonosítása, támadások jelzése, valamint adott esetben kivédése;
- a mesterséges intelligencia a gépi tanulás kombinációjával egyszerű feladatok félautomatikus vagy automatikus felügyeletével történő felhasználása IoT-környezetben is.

A mesterséges intelligencia felhasználásának egyik legnagyobb korlátja az emberi jogok, különösen akkor, ha a mesterséges intelligencia emberekre vonatkozó döntéseket hoz. E tárgyban jelenleg a legvitatottabb témakör a biometrikus adatok kezelése, ezen belül is az arcfelismerés, amelynek betiltását – az emberi jogokat érintő jelentős kockázata miatt – nemzetközi szinten követelik.
„Az AI szelleme már teljesen kiszabadult a palackból, és 2030-ra drámaian megnő a fejlett AI-technológia hasznossága és általános hozzáférhetősége. Ez azt jelenti, hogy gyakorlatilag nincs mód arra, hogy a globális társadalom alapvetően etikátlan rétegeiben kikényszerítsük az etikus felhasználást.
Az etika több évezredes problémája mindig is az volt: Kinek az etikája? Ki dönt, és aztán ki hajlandó megfelelni? Ez egy alapvetően emberi probléma, amelyet semmilyen technikai fejlődés vagy akár egzisztenciális fenyegetés nem fog teljesen megszüntetni.

Alapvetően egymásra vagyunk utalva, és remélhetőleg legalább egy nagy részünk megpróbálja a legjobbat kihozni belőle. De túl sok hatalom és vagyon áll azok rendelkezésére, akik etikátlanul használják a fejlett technológiát, és a felhőn, a dolgok internetén és a nyílt forráskódú szoftvereken keresztüli egyetemes hozzáférés túlságosan megkönnyíti az etikátlan szereplők számára a kihasználást.
Úgy vélem, az egyetlen reális út a nyílt játéktér biztosítása. Ez az egyetemes hozzáférés a technológiához legalábbis mindkét felet egyformán felfegyverezi. Ez lehet, hogy a kölcsönösen biztosított megsemmisítés politikájának felel meg, de a jófiúktól elvenni a fegyvereket csak azt jelenti, hogy többé nem tudják megvédeni magukat a rosszfiúktól."[189]

Németországban a Németország Szociáldemokrata Pártja (SPD[190]), a zöldek és a Német Szabaddemokrata Párt (FDP[191]) a koalíciós megállapodásukba belefoglalták, hogy uniós jogszabállyal kívánják "kizárni" a közterületi biometrikus felismerési gyakorlatot, illetve azt, hogy automatizált állami pontozási rendszerek működhessenek a mesterséges intelligencia segítségével.[192] A francia kormány nem ért egyet a közterületi arcfelismerés betiltásával, véleményük szerint ez a nemzetbiztonságot gyengítené, míg az Európai Parlament felszólítást adott ki az arcfelismerő technológia nyilvános helyeken történő rendőrségi használata, valamint a prediktív rendőri tevékenység betiltására, amely véleményük szerint egy olyan ellentmondásos gyakorlat, amely a mesterséges intelligencia eszközeinek felhasználásával a potenciális bűnözők profilalkotását reméli még a bűncselekmény elkövetése előtt. A prediktív technológia hibái („PredPol") kapcsán már készült statisztikai adatokkal alátámasztott elemzés,[193] illetve egy holland bíróság elrendelte a jóléti csalások felderítésére szolgáló automatizált megfigyelőrendszer azonnali leállítását, mivel az sérti az emberi jogokat.[194] A rendszer célja az volt, hogy megjósolja annak valószínűségét, hogy egy személy szociális segéllyel/adóval kapcsolatos csalást követ el, vagy megszegi a munkaügyi törvényeket, és a rendszer bírósági úton leállíttatása az egyik első alkalom, hogy egy bíróság emberi jogokra hivatkozva leállította a digitális technológiák és a hatalmas mennyiségű digitális információk jóléti hatóságok általi használatát.

---

189 ADAMS, Sam S. – RAINIE, Lee – ANDERSON, Janna – VOGELS Emily A.: Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade; Pew Research Center; June 16, 2021. https://www.pewresearch.org/internet/2021/06/16/experts-doubt-ethical-ai-design-will-be-broadly-adopted-as-the-norm-within-the-next-decade/ (Letöltés ideje: 2022. 02. 22.)

190 Sozialdemokratische Partei Deutschlands

191 Freie Demokratische Partei

192 HEIKKILÄ Melissa: German coalition backs ban on facial recognition in public places; Polico, November 24, 2021. https://www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/ (Letöltés ideje: 2022. 02. 22.)

193 SANKIN Aaron – MEHROTRA Dhruv – MATTU Surya – GILBERTSON Anne: Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them; https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them, December 2, 2021 (Letöltés ideje: 2022. 02. 22.)

194 HENLEY Jon – BOOTH Roberth: Welfare surveillance system violates human rights; Dutch court rules, Wed 5 Feb 2020, https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules (Letöltés ideje: 2022. 02. 22.)

Next generation IT-infrastruktúrák

A következő generációs IT-infrastruktúrák főbb vívmányai például a virtualizáció, a hálózatokba kapcsolt környezetek/alkalmazások, a többszemélyes kapacitások, a testreszabásos lehetőségek biztosítása stb.

Az ezekkel együtt járó kockázatok között várhatóan ott lesznek az alrendszerek esetleges gyengeségei, a konfigurációs hibák, a verzió-gondok, az inkompatibilitás és a biztonsági hiányosságok is. A nagyszámú szereplő által a különféle heterogén rendszerekben kezelt nagy mennyiségű adat a kiberbűnözők számára soha nem látott csábító erőt jelent majd, és előreláthatóan elszaporodnak a bennfentes visszaélések is.

Az új virtualizált infrastruktúrák kölcsönhatásának és architektúrális követelményeinek megértéséhez új módszerek kellenek, a kompetens szaktudás megszerzéséhez pedig időre és sok szakemberre van szükség.

Internet of Bio-Nano Things (IoBNT)

Az IoT-világ számos forradalmi újdonságot hozott, feltehetően még korántsem értünk a folyamat végére, ez pedig különösen igaz a bio-nano tárgyak internetére. Az elképzelések szerint az IoT-eszközök miniatürizálásával és biológiai folyamatokkal kombinálásával a technológia képes lesz majd a sejtek szerkezetének és működésének ellenőrzésére, módosítására, vagy akár újratervezésére is.

Az elképzelések szerint lehetővé válik majd, hogy a biológiai sejteket programozható hordozóként használják. Ez azonban egy olyan lépés lesz a tudományban, amely hatalmas kihívások elé állítja a technológiát, beleértve a kiberbiztonsági, etikai, társadalmi, jogi, gazdasági és politikai szempontokat is, a Covid19-járvány történései pedig bőségesen szemléltetik, milyen támadásokra számíthatnak a jövő jogalkotói a terület szabályozása során.

Azonosítás

Az azonosítás Janus-arcú eszköz, egyrészt bizonyos esetekben alapvető követelmény a bizalom megteremtéséhez, más esetekben pedig a nemléte az, ami szintén alapvető követelmény.

Az IoT-rendszerek esetében kibertérben az azonosítás a kulcspontja az összekapcsolt technológiáknak, egyéneknek, komponenseknek, és minden más azonosítható elemnek.

Az azonosítás szükséges előfeltétele a bizalomnak és a letagadhatatlanságnak is, és ezen a téren az új technológiák megállíthatatlanul törnek előre (pld. biometrikus hitelesítési módszerek) számos jogi és etikai problémafelvetést generálva, például szükséges és arányos-e, valamint megfelel-e a fokozatosság elvének egy iskolai étkezdében a gyermekek azonosítására arcfelismerő rendszert alkalmazni?[195]

Felmerül azonban az anonimitás igénye is, különös tekintettel az emberi jogokra és a privát szféra megsértésének szükségességi-arányossági követelményeire, illetve arra, hogy az egyes szereplők amint személyes adathoz jutnak, azt (üzleti vagy egyéb célból) profilozásra használják fel, ahogy a mindent tudni akaró állam is. A „Big Data" és a mesterséges intelligencia alkalmazásával a természetes személyek azonosíthatósága megnő, és az algoritmusok segítségével az anonim adatok egy része (akár a többsége is) újra személyes adattá válhat.

Kiemelt figyelmet igényel az azonosítás során a biometrikus adatok felhasználása, amelyek közül a legtöbbet emlegetett technológia az arcfelismerés. Ahogy a személyes adatok gyűjtése, tárolása és elemzése egyre szélesebb körűvé és nagyobb volumenűvé válik, egyetlen, önmagában látszólag jelentéktelen személyes „adatmorzsa" más személyes adatokkal – adott esetben akár más adatbázisból átemelt személyes adatokkal – kombinálva már részletes információt nyújthat az érintett személyéről. Ez a hatás érvényesül az arcfelismerő rendszerek esetében is – a különböző adatforrásokból származó adatok kombinációjával az összesített adatokból olyan részletesebb képet lehet alkotni az egyénről, amely alkalmas következtetések levonására, profilozásra és döntések meghozatalára is. Sőt, ezeket az adatokat meg lehet osztani akár harmadik féllel is, az érintett tudta és hozzájárulása nélkül is. A biometrikus adatokból nyert információ lehetővé teszi különleges adatok kinyerését is, például az egyén életkorára, faji, etnikai hovatartozására vagy egészségi állapotára vonatkozóan.

A jogvédők tiltakozását erősíti, és a technológia használatának korlátját jelentheti az is, hogy napjainkban az arcfelismerő technológia pontossága eltérhet bőrszíntől, etnikai hovatartozástól vagy nemtől függően, ez pedig diszkriminációhoz és jogszerűtlen intézkedésekhez vezethet mind az állami, mind a privát szférában. A technológia problémái miatt a Facebook 2021 októberében jelentette be,[196] hogy a jövőben nem használ olyan arcfelismerő rendszereket, amelyek automatikusan felismerik a felhasználókat a fényképeik vagy videóik alapján. A változtatás körülbelül egy milliárd Facebook-felhasználót érint mindaddig, ameddig a jogi környezet nem lesz egyértelműbb.

Az arcfelismerő rendszereket érintő számos kritika mértékét jelzi az is, hogy mintegy 56 jogvédő szervezet szólította fel az Európai Bizottságot, hogy tiltsa meg az arcfelismerő rendszerek alkalmazását a tömeges megfigyelés vonatkozásában. A

---

[195] SHARMA, Suneet: ICO intervenes in nine schools in North Ayrshire which are using facial recognition software to scan faces of pupils in lunch queues; November 8, 2021, https://thestudentlawyer.com/2021/11/08/ico-intervenes-in-nine-schools-in-north-ayrshire-which-are-using-facial-recognition-software-to-scan-faces-of-pupils-in-lunch-queues/ (Letöltés ideje: 2022. 02. 19.)

[196] DANG, Sheila – CULLIFORD, Elizabeth: Facebook will shut down facial recognition system; November 3, 2021, https://www.reuters.com/technology/facebook-will-shut-down-facial-recognition-system-2021-11-02/ (Letöltés ideje: 2022. 02. 22.)

tiltakozás keretében az European Digital Rights (EDRI) nevű csoport a jogérvényesülésért felelős európai uniós biztoshoz címzett felhívásában[197] arra szólította fel az EU intézményét[198], hogy az arcfelismerő technológiák tömeges megfigyelésre való felhasználását kivételek megállapítása nélkül, teljeskörűen tiltsa be.[199]

Következtetések

Az IoT-eszközök legjelentősebb kockázati tényezője a honvédelmi szektor vonatkozásában az, hogy gyors megjelenésük és elterjedésük miatt:

– felügyelet nélkül bekerülhetnek honvédelmi objektumokba,
– az IoT eszközökön felügyeletlen portok aktív kommunikációt folytatnak.

Külön kockázati tényezőként kell figyelembe venni az értékelés során, azt hogy az eszközt ki használja (például minősített adatokhoz való hozzáférés) és mikor.

További kockázati tényezőként figyelembe kell venni a felhasználó életkorát, képzettségét, motivációját a felhasználás tekintetében.

Az eszköz vonatkozásában a kockázatértékelés során figyelembe kell venni azt hogy:

– az eszköz milyen protokollokat és csatornákat használ a kommunikációhoz;
– az eszköz milyen szenzorokkal rendelkezik;
– az eszköz végez-e adattovábbításon kívül adatfeldolgozást;
– az eszköz milyen személyes adatokat kezel;
– az eszköz milyen infokommunikációs szabványoknak felel meg;
– az eszköz szoftverkörnyezetének kialakítása során milyen műszaki irányelveket és EU-ajánlásokat vettek figyelembe.

Felhasznált irodalom:

- (EU) 2018/1725 rendelet 2. cikk (1) bekezdése alapján ezt a rendeletet kell alkalmazni a személyes adatok valamennyi uniós intézmény és szerv általi kezelésére. A rendelet (5) preambulumbekezdése alapján a személyes adatok védelmének az Unión belüli egységes megközelítése és a személyes adatok Unión belüli szabad áramlása érdekében a lehető legnagyobb mértékben összhangba kell hozni az uniós intézményekre, szervekre, hivatalokra és ügynökségekre vonatkozó adatvédelmi szabályokat a tagállamokban a közszféra számára elfogadott adatvédelmi szabályokkal. Amennyiben a (EU) 2018/1725 rendelet rendelkezései ugyanazon elveket követik, mint az (EU) 2016/679 rendelet rendelkezései, ezen két rendelet rendelkezéseit az Európai Unió Bírósága (a

[197] Seeking your support for a specific ban on biometric mass surveillance practices on fundamental rights grounds, 2021. április 1

[198] Commissioner Reynders

[199] Bitport, 2021. 04. 07. https://bitport.hu/nincs-kozeput-az-arcfelismero-technologia-alkalmazasaban (Letöltés ideje: 2022. 02. 22.)

továbbiakban: a Bíróság) ítélkezési gyakorlata szerint egységesen kell értelmezni, különösen mivel a (EU) 2018/1725 rendelet struktúrája az (EU) 2016/679 rendelet struktúrájával egyenértékűnek tekintendő.

- 29. cikk szerinti Adatvédelmi Munkacsoport 9/2011. számú vélemény a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló felülvizsgált ágazati javaslatról (WP180) melléklete: Privacy and Data Protection Impact Assessment Framework for RFID Applications 2011. január 12. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf (Letöltés ideje: 2022. 02. 22.)
- 29. cikk szerinti Adatvédelmi Munkacsoport Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában *„valószínűsíthetően magas kockázattal jár”*-e (WP 248 rev.01), az elfogadás időpontja: 2017. április 4; a legutóbbi felülvizsgálat és elfogadás időpontja: 2017. október 4. https://www.naih.hu/files/WP248_rev01_hu.pdf
- 29. cikk szerinti Adatvédelmi Munkacsoport: 03/2017. számú vélemény a személyes adatok kooperatív intelligens közlekedési rendszerek (C-ITS) keretében történő kezeléséről (WP252).
- 29. cikk szerinti Adatvédelmi Munkacsoport: 05/2014. számú vélemény az anonimizálási technikákról (WP216)
- 29. cikk szerinti Adatvédelmi Munkacsoport: 2/2017. számú vélemény a munkahelyi adatkezelésről (WP249)
- 29. cikk szerinti Adatvédelmi Munkacsoport: 4/2014. sz. vélemény az elektronikus kommunikáció hírszerzési és nemzetbiztonsági célú megfigyeléséről (WP215).
- 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16.
- 29. cikk szerinti Adatvédelmi Munkacsoport: Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához, elfogadás időpontja: 2017. október 3. A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6. (WP251rev.01)
- A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers; An FTC Staff Report, October 21, 2021. https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf (Letöltés ideje: 2022. 02. 21.)
- A személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (elektronikus hírközlési adatvédelmi irányelv), https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU (Letöltés ideje: 2022. 02. 22.)
- ADAMS, Sam S. – RAINIE, Lee – ANDERSON, Janna – VOGELS Emily A.: Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade; Pew Research Center; June 16, 2021. https://www.pewresearch.org/internet/2021/06/16/experts-doubt-ethical-ai-design-will-be-broadly-adopted-as-the-norm-within-the-next-decade/ (Letöltés ideje: 2022. 02. 22.)
- AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation; https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en (Letöltés ideje: 2022. 02. 22.)
- ANI: China launches fresh crackdown on spy cameras in a bid to tighten digital privacy laws; 2021. június 15. https://in.news.yahoo.com/china-launches-fresh-crackdown-spy-170657587.html (Letöltés ideje: 2022. 02. 22.)

- AZ EDPB Nyilatkozata a személyes adatok kezeléséről a COVID-19 járvány kitörésével összefüggésben, elfogadva 2020. március 19-én, pp. 1-2. https://naih.hu/files/edpb-covid-19-nyilatkozat-naih.pdf (Letöltés ideje: 2022. 02. 22.)
- Az Európai Gazdasági és Szociális Bizottság véleménye – Bizalom, a magánélet tiszteletben tartása és biztonság a fogyasztók és a vállalkozások számára a dolgok internetén (2018/C 440/02), https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018IE1038&from=DA (Letöltés ideje: 2022. 02. 22.)
- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L0680&from=hu#d1e893-89-1 (Letöltés ideje: 2022. 02. 22.)
- Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R1725&from=HU (Letöltés ideje: 2022. 02. 22.)
- BBC: Alexa tells 10-year-old girl to put penny in plug socket; 2021. december 28., https://www.bbc.com/news/technology-59810383 (Letöltés ideje: 2022. 02. 21.)
- Bitport, 2021. 04. 07. https://bitport.hu/nincs-kozeput-az-arcfelismero-technologia-alkalmazasaban (Letöltés ideje: 2022. 02. 22.)
- Bundesnetzagentur empfiehlt Vorsicht beim Kauf von smarten Produkten als Weihnachtsgeschenk, Pressemitteilung, Bonn, 20. 12. 2021, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2021/20211220_Smart.pdf;jsessionid=A12415C4E8C492B79A164A86968C316C?__blob=publicationFile&v=https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2021/20211220_Smart.pdf;jsessionid=A12415C4E8C492B79A164A86968C316C?__blob=publicationFile&v=2 (Letöltés ideje: 2022. 02. 21.)
- CERICOLA, Rachel: Ring Neighbors Is the Best and Worst Neighborhood Watch App; June 3, 2021, https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/ (Letöltés ideje: 2022. 02. 22.)
- DANG, Sheila – CULLIFORD, Elizabeth: Facebook will shut down facial recognition system; November 3, 2021, https://www.reuters.com/technology/facebook-will-shut-down-facial-recognition-system-2021-11-02/ (Letöltés ideje: 2022. 02. 22.)
- EDPB 04/2020 sz. iránymutatás a COVID19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használatáról, elfogadás időpontja: 2020. április 21.
- EDPB 3/2019. számú iránymutatás a személyes adatok videoeszközökkel történő kezeléséről, 2.0 változat, elfogadás időpontja: 2020. január 29.
- EDPB 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat, elfogadás időpontja: 2020. október 20.
- EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, version 2.0, adopted on 2021. március 29.

- EDPB Guidelines 02/2021 on Virtual Voice Assistants, version 1.0, adopted on 2021. március 9.
- EDPB Nyilatkozat a kontaktkövető alkalmazások interoperabilitásának adatvédelmi hatásáról, elfogadás időpontja: 2020. június 16.
- Electronic Toy Maker Vtech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act; January 8, 2018. https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated (Letöltés ideje: 2022. 02. 22.)
- ENISA Threat Landscape for Supply Chain Attacks; 2021. július 29; www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (Letöltés ideje: 2022. 02. 22.)
- ENISA Threat Landscape: Sectoral/Thematic Threat Analysis From January 2019 to April 2020; p. 10. https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis (Letöltés ideje: 2022. 02. 22.)
- ENISA: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017. p. 34.
- ENISA: Good practices for Security of Internet of Things in the context of Smart Manufacturing; November 2018. p. 12.
- ENISA: Security and Resilience of Smart Home Environments Good Practices and Recommendations; 2015 December
- ENISA: Security and Resilience of Smart Home Environments Good Practices and Recommendations; 2015 december
- Euronews: US special forces mistakenly assail a factory in Bulgaria; 2021. jún. 2., https://www.youtube.com/watch?v=QzJxzVvI2p8 (Letöltés ideje: 2022. 02. 22.)
- Európai Adatvédelmi Testület: 04/2020 sz. iránymutatás a Covid19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használatáról, elfogadás időpontja: 2020. április 21.
- European Court of Human Rights, Research Division: National security And European case-law, 2013. https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf (Letöltés ideje: 2022. 02. 22.)
- Federal Trade Commission 2020 Privacy and Data Security Update, 3.o. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf (Letöltés ideje: 2022. 02. 22.)
- FLANCHER Balázs: Egy magyar twitterező nyomkövetőt tett egy Kaliforniából feladott csomagba, találják ki, mennyi idő alatt jutott el a magyarországi címzetthez; Telex, 2018. június 18. https://telex.hu/zacc/2021/06/18/csomag-airtag-magyar-posta-egyesult-allamok-magyarorszag (Letöltés ideje: 2022. 02. 22.)
- Ford Motor Co: FordPass; https://play.google.com/store/apps/details?id=com.ford.fordpasseu&hl=hu&gl=US (Letöltés ideje: 2022. 02. 22.)
- HEIKKILÄ Melissa: German coalition backs ban on facial recognition in public places; Polico, November 24, 2021. https://www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/ (Letöltés ideje: 2022. 02. 22.)
- HENLEY Jon – BOOTH Roberth: Welfare surveillance system violates human rights; Dutch court rules, Wed 5 Feb 2020, https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules (Letöltés ideje: 2022. 02. 22.)

- HERN Alex: Microsoft productivity score feature criticised as workplace surveillance; The Guardian, 26 Nov 2020 https://www.theguardian.com/technology/2020/nov/26/microsoft-productivity-score-feature-criticised-workplace-surveillance (Letöltés ideje: 2022. 02. 22.)
- https://nki.gov.hu/it-biztonsag/hirek/agressziv-adatgyujtes-miatt-kapott-birsagot-az-apple-es-a-google/ (Letöltés ideje: 2022. 02. 21.)
- https://www.reuters.com/article/us-usa-trade-china-exclusive-idUSKBN1WM25M (Letöltés ideje: 2022. 02. 22.)
- https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf (Letöltés ideje: 2022. 02. 22.)
- https://naih.hu/hatasvizsgalati-szoftver (Letöltés ideje: 2022. 02. 22.)
- https://www.naih.hu/files/NAIH-2018-356-H_hatarozat.pdf (Letöltés ideje: 2022. 02. 22.)
- https://www.police.hu/adatvedelmi-tajekoztatok/hu!a-rendorsegrol!adatvedelem!altalanos-ugytipusok!allomannyal-kapcsolatos-adatkezelesek!jarmu-koveto (Letöltés ideje: 2021. 02. 22.)
- Hvg.hu: Nagyot kockáztattak a magyar hatóságok a Szputnyik V vakcinával az OGYÉI dokumentumai szerint; 2021. december 23. https://hvg.hu/tudomany/20211223_szputnyik_v_vakcina_ogyei_dokumentumok_hadhazy_akos (Letöltés ideje: 2022. 02. 22.)
- Internet Engineering Task Force (IETF): Terminology for Constrained-Node Networks, 2014 https://www.rfc-editor.org/rfc/pdfrfc/rfc7228.txt.pdf (Letöltés ideje: 2022. 02. 22.)
- KAFKA, Franz: A per (1914); https://mek.oszk.hu/07100/07123/07123.htm (Letöltés ideje: 2022. 02. 21.)
- Kroll: 2021 Data Breach Outlook; https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021 (Letöltés ideje: 2022. 02. 22.)
- Létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény rendelkezéseit.
- Magyar Nemzeti Bank Fenntarthatósági jelentés 2021. https://www.mnb.hu/kiadvanyok/jelentesek/fenntarthatosagi-jelentes/fenntarthatosagi-jelentes-2021 (Letöltés ideje: 2022. 02. 22.)
- Magyarország Mesterséges Intelligencia Stratégiája 2020-2030; 2020. május, p. 26. https://ai-hungary.com/api/v1/companies/15/files/137203/view (Letöltés ideje: 2022. 02. 22.)
- MAUER, Mark: PwC to Spend $12 Billion on Hiring, Expanding Expertise in AI, Cybersecurity; The Wall Street Journal, June 15, 2021. https://www-wsj-com.cdn.ampproject.org/c/s/www.wsj.com/amp/articles/pwc-to-spend-12-billion-on-hiring-expanding-expertise-in-ai-cybersecurity-11623758400 (Letöltés ideje: 2022. 02. 22.)
- NAIH/2019/2471/6. sz. határozat, döntés hivatalból induló adatvédelmi hatósági eljárásban; 2019. június 25. https://naih.hu/files/NAIH-2019-2471-hatarozat.pdf (Letöltés ideje: 2022. 02. 22.)
- Nemzeti Kibervédelmi Intézet: A Solarwinds incidens, Kiberbiztonsági elemzés; https://nki.gov.hu/wp-content/uploads/2021/09/NBSZ-NKI-Kiberbiztons%C3%A1gi-elemz%C3%A9s-a-SolarWinds-incidensr%C5%91l.pdf (Letöltés ideje: 2021. 02. 22.)
- Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones (WP231)

- ORFK érintetti tájékoztató. A VÉDA Közúti Intelligens Kamerahálózat általi adatok kezelése és továbbítása; http://www.police.hu/sites/default/files/2020-03/V%C3%89DA%20%C3%A9rintetti%20t%C3%A1j%C3%A9koztat%C3%B3.pdf (Letöltés ideje: 2021. 02. 22.)
- ORFK érintetti tájékoztató. Büntetőeljárás; http://www.police.hu/sites/default/files/2020-10/bunugy_049_v1.3.pdf (Letöltés ideje: 2022. 02. 22.)
- ORFK érintetti tájékoztató. Gyülekezési törvény hatálya alá tartozó rendezvénybiztosítások; http://www.police.hu/sites/default/files/2019-06/kozrendvedelem_148_v1.1_0.pdf (Letöltés ideje: 2021. 02. 22.)
- ORFK érintetti tájékoztató. Jármű Követő Rendszer adatkezelése (JKR); http://www.police.hu/sites/default/files/2019-12/altalanos_258_v1.0-f%C3%BCggel%C3%A9kkel.pdf (Letöltés ideje: 2022. 02. 22.)
- ORFK érintetti tájékoztató. Jármű Követő Rendszer adatkezelése (JKR); http://www.police.hu/sites/default/files/2019-12/altalanos_258_v1.0-f%C3%BCggel%C3%A9kkel.pdf (Letöltés ideje: 2021. 02. 22.)
- ORFK érintetti tájékoztató. Körözött személyek nyilvántartása; http://www.police.hu/sites/default/files/2020-10/bunugy_245_v1.3.pdf (Letöltés ideje: 2022. 02. 22.)
- ORFK érintetti tájékoztató. Objektív felelősséggel kapcsolatos közigazgatási hatósági ügyek; http://www.police.hu/sites/default/files/2020-03/Kktv.%2021.%20%C2%A7%20objekt%C3%ADv%20felel%C5%91ss%C3%A9g%20%C3%A9rintetti%20t%C3%A1j%C3%A9koztat%C3%B3%20.pdf (Letöltés ideje: 2022. 02. 22.)
- ORFK érintetti tájékoztató. Rendvédelmi alkalmazottak személyügyi alapnyilvántartása; http://www.police.hu/sites/default/files/2019-08/humanigazgatas_255_v1.0.pdf (Letöltés ideje: 2021. 02. 22.)
- ORFK érintetti tájékoztató. Személyügyi nyilvántartás; http://www.police.hu/sites/default/files/2019-06/humanigazgatas_223_v1.1_0.pdf (Letöltés ideje: 2022. 02. 22.)
- ORWELL, George: 1984; Harcourt Brace, New York, 1949.
- PANDURANGAN, V: On taxis and rainbows: Lessons from NYC's improperly anonymized taxi logs; 2014. https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a (Letöltés ideje: 2022. 02. 21.)
- Product Security and Telecommunications Infrastructure Bill, https://bills.parliament.uk/bills/3069 (Letöltés ideje: 2022. 02. 22.)
- Reuters 2021. június 10. https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/ (Letöltés ideje: 2022. 02. 22.)
- SANKIN Aaron – MEHROTRA Dhruv – MATTU Surya – GILBERTSON Anne: Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them; https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them, December 2, 2021 (Letöltés ideje: 2022. 02. 22.)
- SHARMA, Suneet: ICO intervenes in nine schools in North Ayrshire which are using facial recognition software to scan faces of pupils in lunch queues; November 8, 2021, https://thestudentlawyer.com/2021/11/08/ico-intervenes-in-nine-schools-in-north-ayrshire-which-are-using-facial-recognition-software-to-scan-faces-of-pupils-in-lunch-queues/ (Letöltés ideje: 2022. 02. 19.)

- SHERMAN, Justin: Big Data May Not Know Your Name. But It Knows Everything Else, 12. 19. 2021. https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/ (Letöltés ideje: 2022. 02. 21.)
- The European Union Agency for Cybersecurity; https://www.enisa.europa.eu/about-enisa (Letöltés ideje: 2022. 02. 22.)
- VINCENT, James: Canon put AI cameras in its Chinese offices that only let smiling workers inside; The Verge, Jun 17, 2021; https://www.theverge.com/2021/6/17/22538160/ai-camera-smile-recognition-office-workers-china-canon (Letöltés ideje: 2022. 02. 22.)
- ZUBOFF, Shoshana: The Age of Surveillance Capitalism: The Fight For a Human Future At the New Frontier of Power; Public Affairs, New York, 2019, ISBN 9781610395700
- 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16. (továbbiakban: WP223)
- A nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól szóló 7/2015. (XI. 13.) NMHH rendelet 2.§ (1) bekezdés 99.b és 99.c. pontok
- ASHTON, Kevin: That 'Internet of Things' Thing In the real world, things matter more than ideas, 2009. június 22, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf (Letöltés ideje: 2021. 06. 09.)
- Az ENISA: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures; November 2017 alapján
- Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról,- https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=DE (Letöltés ideje: 2022. 02. 21.)
- CASTIGLIONE Aniello – CHOO, Kim-Kwang Raymond – NAPPI, Michele – RICCIARDI, Stefano: Context Aware Ubiquitous Biometrics in Edge of Military Things; IEEE Cloud Computing, 2017/6. pp. 16-20. DOI: 10.1109/MCC.2018.1081072
- Civil Code – CIV. Division 3. Obligations [1427 – 3273.16]. Part 4. Obligations Arising From Particular Transactions [1738 – 3273.16]. Title 1.81.26 – Security of Connected Devices 1798.91.05; https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.26.&part=4.&chapter=&article=, (Letöltés ideje: 2022. 02. 20.)
- COX, Joseph: 'Privacy Protecting' Car Location Data Seemingly Shows Where People Live Work, and Go; 2021. június 10, https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo (Letöltés ideje: 2022. 02. 21.)
- ENISA: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 2017. november, 12. o.
- Európai Uniós kiberbiztonsági Ügynökség – The European Union Agency for Cybersecurity, https://www.enisa.europa.eu/about-enisa / (Letöltés ideje: 2021. 06. 09.)
- HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest, 2018. p. 98.
- https://otonomo.io/ (Letöltés ideje: 2022. 02. 21.)
- https://www.gartner.com/en/information-technology/glossary/internet-of-things (Letöltés ideje: 2022. 02. 20.)

- Internet of Things Cybersecurity Improvement Act of 2020 Sec. 2. (4), 2020. december 4. https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf (Letöltés ideje: 2020. 02. 20.)
- JACK Steward: The Ultimate List of Internet of Things Statistics for 2021. Findstack. 2021. https://findstack.com/internet-of-things-statistics/ (Letöltés ideje: 2022. 02. 21.)
- KOLLÁR Csaba: Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai, Hadmérnök, 2017/4. pp. 146-158.
- Magyarország: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (Letöltés ideje: 2022. 02. 22.)
- RESPERGER István: Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig; Felderítő Szemle, 2013/3. p. 5.; RESPERGER István: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során; Doktori értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2002. p. 45.
- SHAU, Manisha: 7 Applications of IoT in Defence and Military. AnalyticStep, 2021 https://www.analyticssteps.com/blogs/7-applications-iot-defence-and-military (Letöltés ideje: 2022. 02. 20.)
- TÖRÖK Bernát: Információ és kiberbiztonság; Fenntartható biztonság és társadalmi környezet tanulmányok, V. Budapest, 2020. p. 121.

ECK GÁBOR – DR. HABIL. DOBÁK IMRE

A NEMZETBIZTONSÁG INFORMÁCIÓS KÖRNYEZETE

Az információ jelentősége

A nemzetbiztonsági szolgálatok működéséhez kapcsolódóan az „információs" tényező alapvető jelentőségét számos hazai[1] és nemzetközi szakirodalom vizsgálta. A szervezetek tevékenysége mögött meghúzódó „információs" szerep vitathatatlan, hiszen a „szolgálatok alapvetően… információ-szolgáltató szervezetek"[2], amelyek rendeltetéséből adódóan megjelennek az információ megszerzésének, elemzésének-értékelésének és felhasználásának különböző elemei. Az „információ" elméleti megközelítését tekintve közvetlen kapcsolatban áll a nemzetbiztonsági szervezetek alaprendeltetésével, ahol a célok közül a biztonságot érintő döntéshozatalhoz szükséges információk megszerzése, feldolgozása és döntéshozók részére történő átadása emelhető ki, hiszen *„az információ minden döntéshozatal alapvető, integráns eleme"*[3].

Anélkül, hogy e részterületeket tételesen megvizsgálnánk, jó látható, hogy az információk típusai, megjelenési módjai és felületei napjainkban rendkívül dinamikus változáson mennek keresztül, amelyek közvetlen hatással vannak a nemzetbiztonsági szervezetek feladatrendszereire és egyben hatékonyságára is. Ha elvonatkoztatva kitekintünk az információs hadviselés meghatározó területeire[4] (pld. hírszerzésalapú hadviselés, pszichológiai hadviselés, kiberhadviselés), a biztonságot negatívan befolyásoló események előrejelzésének képességére, a dezinformáció kérdéskörének aktualitására, vagy akár a biztonsági technológiák és a kiberbiztonság fejlődésének dinamizmusára, mind mögött a biztonsági ágazat és az „információk" összefüggéseit láthatjuk.

Adat – információ – tudás

Annak érdekében, hogy az információról és a hozzá kapcsolódó tevékenységekről érdemben beszélni tudjunk, fontos a fogalmi meghatározások tisztázása, a határvonalak megjelenítése az adat és az információ között. Olyan, mindenre kiterjedő, egzakt megfogalmazása sem az adatnak sem pedig az információnak nincs, amely a tudomány minden területén megállná a helyét. A

---

1 Többek között: JÁVOR Endre: A hír, az adat, az információ és a dokumentáció fogalma, helye, szerepe a döntéshozatalban; Nemzetbiztonsági Szemle, 2017/3. pp. 36-60., valamint VIDA Csaba: A nemzetbiztonsági tevékenység szerepe a társadalomban (Gondolatok arról, hogy miért van szükség nemzetbiztonsági szolgálatokra); Hadtudomány, 2015/E. pp. 221-234.

2 VIDA (2015) i. m.

3 JÁVOR (2017) i. m. p. 41.

4 LIBICKI, Martin C. The Convergence of Information Warfare; Strategic Studies Quarterly, 2017/1. pp. 49–65. http://www.jstor.org/stable/26271590. (Letöltés ideje: 2022. 05. 20.)

kifejezések mindennapi használata során sok esetben az adat és az információ egyenértékűek, egymás szinonimájaként használatosak, amely hibás megoldás. Alaposabban megvizsgálva azonban jelentős különbségek vannak a két fogalom között. Ez a különbség már a Magyar Nyelv Értelmező Szótára által adott meghatározásokból is érzékelhető, amely szerint az adat: valaminek megmagyarázására, megvilágítására, jellemzésére vagy kiegészítésére közölt tény, részlet; adalék, illetőleg valamely dologra vagy tárgykörre vonatkozó, ismert, írásban nyilvántartott tény.[5] Az információ valamely személyre vagy ügyre vonatkozó tájékoztatás, felvilágosítás.[6] Bencsik Andrea úgy véli, hogy az adat ítélet és összefüggés nélküli tárgyilagos tény, míg az információról azt gondolja, hogy az úgy keletkezik, hogy az adatokon végrehajtott tevékenységeken keresztül, úgymint elemzés, kategorizálás, összegzés, új hozzáadatott értéket teremtünk.[7]

Tovább vizsgálva a definíciókat megállapítható, hogy az adatok rendezetlen és strukturálatlan tények, amelyek rendelkeznek analitikai szempontból értékkel. Az információ pedig az adatokból strukturálást és feldolgozást követően elérhető következtetések, amelyek további elemzésre is alkalmasak. Az adatnak önmagában általában nincs jelentősége, nem használható döntéshozatalra, ellentétben az információval, ami önállóan is hangsúlyos, és képes a döntési folyamatok támogatására. Ezek alapján megállapíthatjuk, hogy az adattól függ az információ, de az információ nincs hatással az adat tartalmára. Nemzetbiztonsági szempontból vizsgálva az adat és az információ viszonyát megállapítható, hogy az adat a valós tények megjelenési formája, míg az információ az az adat, amely átesett az értékelő-elemző feldolgozásom[8].

Az adat és információ párosa után juthatunk el a tudáshoz, amely az adatok rendelkezésére állásának biztosítását követően, az információ kinyerése, megszerzése érdekében folytatott tevékenységek során keletkező, rendelkezésre álló többlet, amelyhez továbblépési akarat és lehetőség is társul[9]. Szeleczki Zsolt párhuzamot von a tudás, vagyis az olaj feltárása és kitermelése között. „*Az adatoknak van egy vastag rétege, és egy kicsit vékonyabb információs rétege (amelyet alkalmazott adatoknak vagy egymással összefüggésben álló adatoknak lehet nevezni) közöttünk és a számunkra szükséges tudás viszonylag vékony rétege között. Még azon a rétegen belül,*

---

5 Magyar Nyelv Értelmező Szótára: Az adat meghatározása. https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/a-a-1BFAF/adat-2-1C1E3/?list=eyJmaWx0ZXJzIjogeyJNVSI6IFsiTkZPX0xFWF9MZXhpa29ub2tfMUJFOEIiXX0sICJxdWVyeSI6ICJhZGF0In0, (Letöltés ideje: 2022. 05. 15.)

6 Magyar Nyelv Értelmező Szótára: Az információ meghatározása https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/i-i-31843/informacio-3225D/?list=eyJmaWx0ZXJzIjogeyJNVSI6IFsiTkZPX0xFWF9MZXhpa29ub2tfMUJFOEIiXX0sICJxdWVyeSI6ICJpbmZvcm1cdTAwZTFjaVx1MDBmMyJ9 (Letöltés ideje: 2022. 05. 15.)

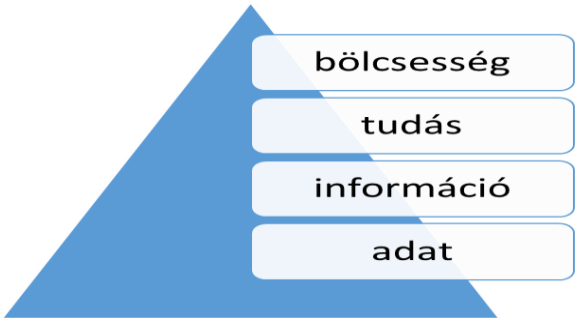
7 Bencsik Andrea: A tudásmenedzsment emberi oldala; Z-Press Kiadó Kft. Miskolc, 2009. p. 17.

8 Vida Csaba: A hírszerzési ágak elemző-értékelő megközelítése; Felderítő Szemle, 2016/3. pp. 77-94.

9 Kent, Sherman: Strategic Intelligence for American World Policy, Princeton University Press, Princeton, 2015. https://doi.org/10.1515/9781400879151 (Letöltés ideje: 2022. 05. 30.)

amelyet elérni kívánunk, van a hasznos tudás – ugyanaz, mint a kőzetrétegen belül az olaj."[10] Manuel Castel szerint *„A tudás pedig olyan állítások halmaza, amelyek abból a folyamatból születnek, amikor az emberi elmét egy megfigyelhető jelenség megértésére használjuk."*[11]

A tudás, az információ és az adat közötti viszonyrendszert leginkább az úgynevezett DIKW[12]-modellel vagy piramissal lehet megérteni, ábrázolni. A piramis alapzatát képezi az adat, felette az információ, illetve a tudás helyezkedik el, a piramis csúcsa a bölcsesség, amely a jövőre vonatkozó előrejelző képességet testesít meg.



1. ábra: DIKW-piramis
(saját szerkesztés)

A modell piramis formában való megjelenítése jól ábrázolja az alkotóelemek egymáshoz való hierarchikus viszonyát. Ezek ismeretében kijelenthető, hogy a jövő, és annak minél pontosabb előrejelzése nem képzelhető el a rendelkezésre álló adatok, információk, és a belőlük fakadó tudás ismerete nélkül.

Adatok az információs térben, az OSINT[13] és a SOCMINT[14] jelentősége

Az információs technológiában bekövetkezett változások – elsősorban a virtuális tér tágulásával és az abban lévő szereplők körének kiterjesztésével – a mindenki számára elérhető adatok, információk számát megsokszorozták. Az információkat nem csak használjuk, hanem magunkról is egyre több információt osztunk meg. A virtuális térben való létünk sok esetben összemosódik valódi életünkkel, és virtuális közösségeink sokszor szinte követelik, hogy adatot, információt osszunk meg, aminek mi készségesen eleget is teszünk, nem törődve annak esetleges következményeivel. Ugyanakkor *„minél jobban összekapcsolódik az életünk a világhálóval, annál inkább összeolvad a valós és a virtuális identitásunk, annál több releváns információ kerül*

---

[10] SZELECZKI Zsolt: A tudás menedzsment koncepciója és háttere; Vezetéstudomány, 1999/12. p. 22. http://unipub.lib.uni-corvinus.hu/5172/1/VT_1999n12p22.pdf (Letöltés ideje: 2022. 05. 10.)

[11] CASTELLS, Manuel: A tudás világa; Napvilág Kiadó, Budapest, 2006. p. 137.

[12] Data, Information, Knowledge, Wisdom (adat, információ, tudás, bölcsesség)

[13] Open Source Intelligence – Nyílt forrású információgyűjtés

[14] Social Media Intelligence – Közösségi médiából történő információgyűjtés

megosztásra, és így azok nyomon követhetőbbé és elérhetőbbé válnak a lehető legteljesebb elemzés elkészítéséhez."[15]

Az online közösségi média, annak térhódításával párhuzamosan számos kutatás részévé vált. Mind a műszaki, mind a társadalomtudományi területen széles kutatói közösségek fordultak a digitális térben formálódó különböző kapcsolatrendszerek, kapcsolatok vizsgálatának irányába. A globális közösségi felületek ugyanakkor a biztonságért felelős ágazat érdeklődését is felkeltették, hiszen számos biztonsági esemény közvetlenül kapcsolódik a virtuális térben megjelenő információkhoz. Gondoljunk csak a terrorizmus jelenségére, a szervezett bűnözői csoportok működésére, de kapcsolódása akár a hibrid hadviselés (HW – Hybrid Warfare) eszköztárában is látható. Gondolunk itt a hadviselő információs tevékenységére (pld. propaganda, félretájékoztatás, dezinformáció, befolyásolás).[16] Az itt megjelenő információk, kapcsolatok, összefüggések megismerése, elemzése így egyre fontosabbá válik a nemzetbiztonsági szervezetek munkája során. Mindezekkel elsősorban az OSINT és a SOCMINT hírszerzési ágakban találkozhatunk, amelyek azonban főként konkrét eseményekhez, folyamatokhoz, valamint személyekhez köthető információs igények kiszolgálásához kapcsolódnak, és nem a személytelen, azonban mögöttes folyamatokra utaló nagytömegű adatok vizsgálatára és összefüggések feltárására irányulnak.

A SOCMINT viszonylag fiatal területnek tekinthető. A közösségi oldalak térhódításával párhuzamosan fejlődött, és megoldásai, módszerei folyamatosan illeszkednek a kibertér változó viszonyaihoz. Az információgyűjtési ág azonban napjainkra már a humán, illetve a technikai terület sajátos egyvelegének tekinthető. Módszerei között különösen fontossá vált az információk elemzésének, az összefüggések feltárásának szerepe.

A közösségi felületeket tekintve számos kategória definiálható, amely a kommunikáció irányát jelentheti. Ezek közé sorolható például az egyének közötti kommunikáció, az egyén–csoport irányú kommunikáció vagy akár például a reklám-/üzleti célú, széles tömegek felé irányuló kommunikáció. Utóbbi kategóriához sorolható akár a politikai, de akár a média irányából megjelenő kommunikáció is. A kategorizálás lehetősége számtalan, hiszen az emberek, csoportok közötti kommunikáció egy része helyeződött át a kibertérbe, sőt sajátos elemként fontossá vált a közösségi térben történő állandó láthatóság szerepe is. A háttérben természetesen jelen van a kommunikáló által felvállalt valós személyiség, illetve fiktív adatokkal való megjelenés lehetősége is.

A nemzetbiztonsági szervezetek esetében az érdeklődés alapesetben egyének, illetve adott csoportok irányába mutatkozhat meg, amely adatokat más forrásokkal összevetve kaphatnak teljesebb képet. Fontos hangsúlyozni, hogy a közösségi oldalakat használók gyakran adataikat bárki számára nyíltan elérhető módon teszik közzé, így ezen információk megismerése a hagyományos OSINT kategóriájába sorolható. (Ugyanakkor érdekes kérdést vett fel az, hogy a másokról – esetleg azok

---

[15] LOMBARDI, M. – ROSENBLUM, T. – BURATO, A.: From SOCMINT to Digital Humint: re-frame the use of social media within the Intelligence Cycle; Fondazione de Gasperi, 2015. p. 2.

[16] A témakörben lásd: KIS Álmos Péter: A hibrid hadviselés természetrajza, Honvédségi Szemle, 2019/4. p. 31.

beleegyezése nélkül – nyilvánossá tett információk köre, ami álláspontunk szerint teljes mértékben megfelelhet a nemzetbiztonsági célú felhasználásnak, egyéb, akár büntetőeljárásban történő felhasználása milyen jogi aggályokat vethet fel.)

A hagyományosnak tekinthető információgyűjtési ágakhoz (pld. HUMINT, SIGINT) viszonyítva az infokommunikációs felületek nyílt forrásait kiaknázó fenti területek – nemzetbiztonsági szemmel – ugyanakkor sajátos előnyöket hordoznak magukban, amelyek közül jelen tanulmányban az alábbiakat tartjuk kiemelésre érdemesnek:

- Az internetnek köszönhetően lehetővé vált az adott konfliktusoktól, eseményektől távoli, biztonságos térségekből történő információgyűjtés lehetősége. (Ezek végrehajtásának kockázata jóval alacsonyabbnak tekinthető a hagyományos információszerző tevékenységekhez képest.)
- Ide sorolható a rendkívül dinamikus biztonságpolitikai környezeti változások gyors nyomon követhetősége, a globális média gyakran humán forrásokat is igénybe vevő kezdeti információinak felhasználása.
- A technológiai megoldások további előnyeként jelenik meg, hogy a megfelelő források felkutatása, az információgyűjtési irányok megváltoztatása gyorsabb, mint a HUMINT-képességek kiépítésének folyamata. A rendkívül dinamikusan változó világunkban ennek kiemelt jelentősége lehet.
- Kiemelhető az információgyűjtés „szakosodásának" lehetősége. Ilyen például a SOCMINT, ahol a kapcsolatrendszerek, összefüggések, valamint a közösségi oldalakon jelölt információk mögött meghúzódó valós emberi aktivitások más forrásokhoz képest gyorsabban válhatnak megismerhetővé.
- Széles körben elérhetővé váltak azok a nyílt technikai megoldások (szoftverek), amelyek (az OSINT kategóriáján belül), lehetővé tehetik egy-egy biztonsági esemény akár titkosszolgálati mélységű elemzését. Az információforrások széles köre (ide sorolva mind a nyílt és a fizetős adatbázisokat) megfelelő elemzési szakértelemmel, és akár egyéb szakterületek szakértőinek bevonásával korábban nem elérhető elemzések elkészítését teszik lehetővé. A nyílt források mélyebb vizsgálata a napjainkban erősödő dezinformáció jelensége során is az egyik lehetséges megoldásként jelenik meg, rávilágítva egy-egy esemény és kapcsolódó forrásai ellentmondásaira. Gyakran említett példaként emelik ki a „Belingcat" oldal és a mögötte lévő szakértők tevékenységét, akik például az orosz–ukrán háború kapcsán megjelenő egyes információk valóságtartalmának vizsgálata kapcsán váltak közismertté.[17]
- Lehetővé vált a biztonsági ágazaton kívül keletkezett, nyílt forrásként megjelenő, ugyanakkor hitelesnek tekinthető információk bevonása. Ide sorolható, hogy a kibertérben megszerezhető nyílt információk ma már az üzleti szereplők számára sem nélkülözhetetlenek, a versenytársak és a piaci változások monitorozása általánosan alkalmazott megoldások, és az ezekre épülő profitorientált piaci szegmensek (információbórkerek) térhódítását láthatjuk.

[17] https://www.bellingcat.com/news/2022/04/14/russias-kramatorsk-facts-versus-the-evidence/ (Letöltés ideje: 2022. 05. 18.)

A digitális adatok hatása az információgyűjtés egyéb területeire

A Datareportal adatai szerint az internet használók 93,4%-a használja valamelyik közösségi média felületét. 2021 januárja és 2022. januárja között 424 millió új felhasználó csatlakozott valamelyik platformhoz, így a közösségi médiát aktívan használók száma 2022 januárjában elérte 4,62 milliárd főt világ szerte. Ez azt jelenti, hogy a Föld lakosságának 58,4%-a jelen van ezeken a platformokon.[18] A felhasználók száma és a kapcsolódó digitális forrásokban megjelenő információk tömege jól mutatják, hogy a technológiai környezet változása hatással kell, hogy legyen az információgyűjtés különböző területeire, bizonyos elemeiben érinthetik, a kibertér irányába elmozdulásra késztethetik a hagyományosan a HUMINT-hoz köthető egyes elemeket is (pld. kapcsolattartás).

Kérdésként merülhet fel, hogy a technológiai környezet változása hogyan érintheti a humán forrásokhoz köthető területet, hiszen ezek létrehozása és működtetése, az emberi természetből adódóan ugyanazokon a tulajdonságokon alapul, mint évezredekkel ezelőtt. A meg nem értettség, sértődöttség, a pénz, az emberi ego, a zsarolhatóság, vagy akár az ideológiai jellegű szempontok napjainkban is jelen vannak. Ennek jelentősége csupán annyit változott, hogy ezek már nem csak a valós térben megjelenő személyek közötti kapcsolatokban vannak jelen, hanem a kibertérben is érezhetőek. Nem egyszerűen a hálózatok adta lehetőségekre érdemes gondolni, hanem a digitális világ és a kibertér komplexebb összefüggéseire[19], amelyek hatást gyakorolhatnak a jövő HUMINT-műveleteire is. Ide sorolható többek között, hogy:

- A digitális világ lehetővé tette a HUMINT-területeken dolgozók számára, hogy nagy távolságokra, biztonságos módon információkat továbbítsanak, csökkentve ezzel a kockázatos személyes találkozók számát.
- A közösségi médiafelületek összetett, több irányban is felhasználható sajátos lehetőségeket teremtettek. Amellett, hogy ezek a platformok a nyíltan közzétett információk révén kiegészítő adatokkal szolgálhatnak, jó felületei lehetnek a tippkutatásnak, a kiválasztásnak, közvetve támogathatják adott műveletek, illetve tevékenységek eredményességét is. Ugyanakkor, míg e tevékenységek a „való világban" szigorú szabályok mentén mozognak, addig a virtuális térben történő hasonló mozzanatok igen alulszabályozottak.
- A digitális adatok lévén – a civil társadalomhoz hasonlóan – az önkéntesen megosztott adatok révén lehetővé vált személyek mozgásának bizonyos mértékű nyomon követése, kiegészítő információk elérése, akár eseményekhez kötötten.
- A technológiai fejlődés ugyanakkor a HUMINT végzésére is befolyást gyakorolhat, gondoljunk csak a rólunk elérhető adatokra (vagy annak indokolatlan hiányára), a határok átlépéséhez kapcsolódóan a biometria felértékelődő szerepére, de gondolhatunk a digitális eszközök által hagyott nyomokra is.

---

[18] https://datareportal.com/global-digital-overview#:~:text=Roughly%204.66%20billion%20people%20around,over%20the%20past%20twelve%20months (Letöltés ideje: 2022. 04. 20.)

[19] GIOE, David V.: „The More thing Change". HUMINT in the Cyber Age; In: DOVER, Robert – DYLAN, Huw – GOODMAN, Michael S. (eds.): The Palgrave Handbook pf Security, Risk and Intelligence; Palgrave Macmillan, London, 2017. pp. 213-227.

– A digitális világban nem feledkezhetünk meg a saját oldalon álló emberi tényező szerepéről és annak megbízhatóságáról sem. Az elmúlt évtizedek kiszivárogtatási botrányai[20] mind ennek a kérdésnek a sérülékenységét jelentették, amelyre válaszul felértékelődtek az egyes országok biztonságtudatosítási (informatikai, információ és operatív) és kiberbiztonsági programjai.
– A digitális világ rejtett megoldásai segíthetik, de akár meg is nehezíthetik az illegális tevékenységek feltérképezését. Gondoljunk az illegális tevékenységeket végzők (szervezett bűnözői csoportok, terroristák, ipari kémkedéssel foglalkozók) megjelenésére, akik konspirált módon történő működésére az elmúlt években, a médiában is számos példát láthattunk.[21] A közvetlen kommunikáció kerülése, a jelek, üzenetek rejtése, vagy akár sajátos megoldása (számítógépes játékok, üzleti üzenetek) rendkívüli módon megnehezíthetik az adott nemzetek számára az illegális tevékenységet végzők felderítését.

Lehetséges új irányként vizionálható a hátérben tömegesen meghúzódó, a metaadatok kategóriájába sorolható adatok és információk felhasználása, amelyek szélesebb következtetések levonására, előrejelzések megfogalmazására lehetnek alkalmasak. A jövőre kitekintve kérdésként merülhet fel, hogy a tömeges információs halmazból milyen módszerek és megoldások segíthetik majd a valós információk kiszűrését, azok elemzését-értékelését, hiszen ezek kiemelten fontosak a nemzetbiztonsági szereplők számára.

Itt említhető az ún. Crowdsourcing Intelligence módszere, amely arra épít, hogy a különböző közösségek tagjait bevonja az információ megszerzésébe, esetleg annak rendszerezésébe. A „crowdsourcing" szóösszetételben az angol „crowd" (tömeg) és az „outsourcing" (kiszervezés) kifejezéseket láthatjuk, amelyek jól jelzik a kategória lényegét, vagyis a feladatok feldarabolását, széles körnek történő kiosztását (kiszervezését), és a nagyszámú, elkülönült szereplők bevonása eredményeként a részeredményekből közös „eredménytermékek" létrehozását.[22] Maga a crowdsourcing, amely fogalma Jeff Howe nevéhez köthető, aki 2006-ban megjelent cikkében[23] használta, alapvetően üzleti szemléletű megközelítéssel, főként az informatika területén kutatott, de napjainkra egyéb területeken (pld. társadalomtudományok) is teret nyert.[24]

A Crowdsoursing Intelligence alkalmazása meglepő módon jóval az internet elterjedése és az online térben történő adattovábbítás térnyerése előtti időre datálható. Elég csak a 1960-as években az Amerikai Egyesült Államok ittas járművezetést

---

[20] SNOWDEN, Edward – GREENWALD, Glenn: A Snowden-ügy; HVG Könyvek, 2014. ISBN: 9789633041833
Julian Assange, https://www.britannica.com/biography/Julian-Assange (Letöltés ideje: 2022. 05. 17.)

[21] EL HOUDAIGUI, Rachid: Terrorism and new technology; https://gnet-research.org/2021/06/24/terrorism-and-new-technology/ (Letöltés ideje: 2022. 05. 18.)

[22] A fogalom meghatározásai kapcsán lásd: STOTTLEMYER, Steven A.: HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence; International Journal of Intelligence and CounterIntelligence, 2015/3. pp. 578-589, DOI: 10.1080/08850607.2015.992760

[23] HOWE, Jeff: The Rise of Crowdsourcing, Wired, Jun 1. 2006, Letöltés helye: https://www.wired.com/2006/06/crowds/ (Letöltés ideje: 2022. 05. 24.)

[24] Uo. p. 580.

visszaszorítani kívánó, vagy a nyolcvanas években induló és a lakosság egymásra figyelésére alapozó bűnmegelőzési kampányaira gondolni. Igaz, valódi értéke az internet széles körű elterjedésével és az infokommunikációs eszközök mindennapi életünkben betöltött szerepének emelkedésével, a közösségi platformok elterjedésével erősödött fel.

Nemzetbiztonsági értelmezésben S. Stottlemyre fogalmazza meg írásban[25], hogy a Crowdsourcing Intelligence olyan információk gyűjtését jelenti, amelyeket eredetileg emberek gyűjtöttek össze[26] és nyílt forrásokhoz kapcsolódnak. Ezen tevékenységeket hagyományosan az OSINT és a HUMINT fedik le, a Crowdsourcing Intelligence azonban eltérő sajátosságokkal bír. Amíg az OSINT valóban a nyílt információk és megoldások mentén működhet, addig a HUMINT során már az információgyűjtés szándékának és résztvevőinek elfedése sajátos technikák és megoldások alkalmazását igénylik. A Crowdsourcing Intelligence során pedig a kéréseket nyíltan kell megfogalmazni egy széles résztvevői kör (tömeg) felé.[27] Igaz, hasznosságát a biztonságért felelős szervek is felismerték, ugyanakkor a benne rejlő kockázatokat (pld. információgyűjtés irányának akár nyílt megjelenése) és átfogó nemzetbiztonsági alkalmazásának technikai és jogi aspektusait még vizsgálni kell.

Infokommunikációs környezetünkben egyre több olyan adattal találkozhatunk, amelyek nem a hagyományosnak tekinthetőek, előzőekben ismertetett területeken jelennek meg, de adataik révén mégis közvetlenül segítik a biztonság témakörében végzett elemző-értékelő munka eredményességét.

A napjaink infokommunikációs környezetéhez kapcsolódó társadalomtudományi kutatások egyik problémájaként érezhető, hogy szűkösek, illetve széles körben nem érhetőek el azon infokommunikációs környezethez kapcsolódó, személyes adatokat nem tartalmazó adathalmazok, amelyek elősegítenék számos folyamat tudományos, nagytömegű adatokon alapuló vizsgálatát. Érdemes ezeket a személyes adatoktól mentes adatokat ún. metaadatokat is egy kicsit jobban megvizsgálni annak érdekében, hogy azok biztonsági célú felhasználása a társadalmi elfogadottság szempontjából helyénvalók legyenek. A metaadatok lényegében és leegyszerűsítve olyan „kísérőadatok", amelyek kapcsolódó információval látnak el bennünket az alapadatokról. Ezek az adatok kiegészítik az adatról rendelkezésre álló információkat, ilyen lehet például az adat forrása, létrehozója, mérete, típusa, földrajzi elhelyezkedése, létrehozásának ideje, illetőleg az ezekben alkalmazott módosítások, változtatások, anélkül, hogy az alapadat tartalmában változtatást hoznának.[28] Ezen adatok köre a különböző technológiák mentén egyre nagyobb méreteket ölt, és jól látható, hogy napjainkat, és már közeli jövőnket az adatok, információk megosztása, az azokkal történő gazdálkodás, és a hozzájuk kapcsolódó szervezési feladatok jelentősen befolyásolják mind gazdasági, társadalmi, és nem utolsó sorban biztonsági vonatkozásban.

Számos példa emelhető ki, így az általános elterjedt térinformatikai megoldások mára már alapnak tekinthetőek, a profilalkotás végrehajtását is technikai megoldások

---

25 STOTTLEMYER (2015) i. m. pp. 578-589.
26 Uo. p. 583.
27 Uo. p. 585.
28 KRANZ, Garry: Metadata, https://www.techtarget.com/whatis/definition/metadata (Letöltés ideje: 2022. 05. 24.)

(pld. földrajzi profil térképi megoldásai) segítik.[29] Ugyanakkor rendkívüli módon fejlődő területként tekinthetünk az egyre hatékonyabb videomegfigyelő, és az azzal egybeolvadó arcfelismerő technológiákra, amelyeket kormányok és napjainkban már számos szervezet használ. A technológiákra, amelyek biztosíthatják az emberek rendkívül gyors azonosítását, mozgásuk nyomon követését. Legelterjedtebb példaként Kínát emelte ki a szakirodalom az állampolgárok viselkedésének figyelemmel kísérése kapcsán, de a biztonsági szempontok mentén egyre szélesebb körben kerülnek alkalmazásra például repülőtereken, egyéb biztonsági létesítményekben.[30] A megfigyelésnek a mesterséges intelligenciával összefonódó módja jól mutatja, hogy a technológiai lehetőségek már jóval túlmutatnak a társadalom általánosan elfogadott értékrendjén és az aktuális jogszabályi kereteken, így a biztonság növelése vs. adatvédelem és szabadságjogok témakörében megjelenő társadalmi vitákkal párhuzamosan a jogi keretek szabályozása is szükségessé válhat. A mesterséges intelligencia egyre inkább meghatározó térhódítása kapcsán, mint Peter Engelke kifejti tanulmányában[31], amellett, hogy lehetőségeket nyújt a bűnüldözés és a bűncselekmények megelőzése során, és számos területen (autonóm járőrözés, nyomkövető rendszerek, előrejelzési eszközök) már jelenleg is használatos, alkalmazásuk aggodalmakat kelthet a megfigyeléstől való félelem, az adatvédelem, vagy akár a nem átlátható, mesterséges intelligencia által meghozott döntések terén.

A mesterséges intelligencia mindennapi életünket egyszerűbbé tevő előnyös megoldásai mellett látható a technológiával szemben megjelenő társadalmi bizalmatlanság, *„a társadalom működése során keletkező nagy mennyiségű adat etikátlan felhasználásával való szembesülés, vagy akár az egyre nagyobb mértékben digitalizálódó társadalom manipulálhatóságának tapasztalata.”*[32]

A dezinformáció jelenségének kihívásai

A kibertér online felületei az elmúlt időszakban robbanásszerűen felerősítette a dezinformálás jelentőségét, a széles csoportok adott érdekek mentén történő manipulálásának, befolyásolásának lehetőségeit. Az álhírek, félretájékoztatás és dezinformáció olyannyira átszövik mindennapjainkat, hogy még a szakavatott nemzetbiztonsági szervezeteket is kihívás elé állítja a valós, valótlan információk és a szándékos dezinformációs elemek elkülönítése. A kérdéskör komplexitását jól mutatja annak fogalmi meghatározása is, ahol a félretájékoztatás (misinformation) és a dezinformáció (disinformation) elkülönítése során a szándékosság és a befolyásolási szándék elemei kapnak kulcsszerepet. Amíg a félretájékoztatás során a valótlan híreket károkozási szándék nélkül osztják meg, addig a dezinformáció (disinformation) során a hamis, vagy akár módosított információk megosztása tudatosan, valamilyen politikai, biztonsági, vagy akár gazdasági cél elérése érdekében

[29] MÁTYÁS Szabolcs: Az elemző-értékelő munka gyakorlati aspektusai; NKE KTI, Budapest, 2020. pp. 7-11.

[30] ENGELKE, Peter: AI, Society, and Governance: An Introduction, Atlantic Council; 2020. https://www.jstor.org/stable/resrep29327 (Letöltés ideje: 2022. 05. 24.)

[31] ENGELKE (2020) i. m.

[32] SZABÓ Hedvig – DOBÁK Imre: Az információs társadalom nemzetbiztonsága; Nemzet és Biztonság, 2021/2. p. 102. doi: 10.32576/nb.2021.2.7

történik, és adott fél befolyásolására irányulhat.[33] A biztonsági szereplők esetében a dezinformáció kap különös jelentőséget, amely az Európai Bizottság értelmezésében *„olyan igazolhatóan hamis vagy félrevezető információ, amelyet gazdasági haszonszerzés vagy szándékos megtévesztés céljából hoznak létre, hoznak nyilvánosságra és terjesztenek, és amely kárt okozhat a közérdeknek."*[34]. A jelenség elválaszthatatlan részeként tekinthetünk ugyanakkor a propagandatevékenységek bizonyos elemeire is, hiszen mindezek a hibrid hadviselés során más eszközökkel együtt kerülhetnek alkalmazásra.

A jelenség a biztonsági ágazat részéről megjelenő információgyűjtés és elemzés tevékenységére közvetlen hatást gyakorol, amely a nemzeti szintű gondolkodás mellett mind az EU, mind a NATO szintjén nyomon követhető. Amellett, hogy a dezinformáció a nemzetbiztonsági és katonai gondolkodásban nem új jelenség, hiszen a másik fél tudatos megtévesztése mindig is jelen volt a hadviselésben, az elmúlt időszak fegyveres konfliktusai és a társadalmat elérő infokommunikációs környezet, a közösségi platformok biztosította lehetőségek felértékelték annak hadviselésben játszott szerepét. A jelenség térhódítása mögött a hadviselés változása és a hibrid hadviselés előtérbe kerülése követhető nyomon, ahol az emberi, társadalmi környezet, a lakosság gondolkodásának befolyásolása válik meghatározóvá.[35] A kibertérben történő dezinformáció terjedésére az elmúlt időszakban számos példát láthattunk, amelyek alátámasztották a jelenség gyors alkalmazkodását a digitális felületekhez (közösségi üzenetek, mémek, deep fake megoldások), bevonva a hagyományos katonai szereplőkön túlmutató nem állami szereplőket is. Kiváló példa erre a jelenleg zajló orosz-ukrán háború kibertérben történő felerősödése, amikor a harci cselekmények saját szemszögből való magyarázatán túl, állami vezetők el nem hangzott nyilatkozatain[36] és polgári személyekkel kapcsolatos hamis információkon[37] keresztül törekednek befolyásolni a közvéleményt.

A nemzetbiztonsági szereplők számára ennek megfelelően egyre nagyobb feladatot jelent a valós információk kiszűrése, amely a digitális, nyíltan elérhető forrásokon túl az információszerzés egyéb forrásainak és komplex alkalmazásának felerősödését jelenthetik (összadatforrású információszerzés).

Kiemelésre érdemesnek tartjuk az OSINT területét, amely amellett, hogy az információk tömeges megszerzése és elemzése terén jelentett fordulópontot, szerepet kaphat a valós és valótlan információk elkülönítésében (fact-checking – tényellenőrzés) is.

---

[33] DOBÁK Imre: A dezinformáció – napjaink kiemelt kihívása; Katonai Jogi és Hadi Jogi Szemle, 2022/1. http://epa.oszk.hu/02500/02511/00020/pdf/EPA02511_katonai_jogi_szemle_2022_1_093-124.pdf (Letöltés ideje: 2022. 05. 24.)

[34] A BizottságKözleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Európai megközelítés az online félretájékoztatás kezelésére, Európai Bizottság, Brüsszel, 2018.4.26. COM (2018) 236 final.

[35] PORKOLÁB Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? Hadtudomány, 2015/3-4. p. 42.

[36] https://www.bbc.com/news/technology-60780142 (Letöltés ideje: 2022. 05. 18.)

[37] https://www.bbc.com/news/topics/cjxv13v27dyt/fake-news (Letöltés ideje: 2022. 05. 18.)

Az erre szakosodott weboldalak[38] és kapcsolódó digitális technikák (pld. képelemzés, metaadatok elemzése) az álinformációk kiszűrése kapcsán kaphatnak szerepet, továbbá a biztonságtudatosítás tevékenysége révén segíthetik a társadalom álhírekkel szembeni ellenállóképességét.

Összefoglalás

Összegzésképpen elmondható, hogy napjainkban a digitális világ, a világháló és ezen belül is a közösségi média szerepe átformálja az információgyűjtés területeit. Mind az OSINT, a SOCMINT és a HUMINT tevékenysége is módosulóban van, mivel folyamatosan alkalmazkodniuk kell a változó külső technológiai környezethez. A változás ugyanakkor nem csupán fejlődést jelenthet, hanem az információgyűjtési területek közötti határok elmosódásával is számolni kell.

A virtuális térben megjelelő, illetve az ott keletkező nemzetbiztonsági értékkel rendelkező hatalmas adatmennyiség a klasszikus elemzési módszerekkel egyre nagyobb kihívást jelent a biztonsági szolgálatok számára. Folyamatosan keresni kell a megjelenő technikai, technológiai újdonságok biztonsági felhasználásának lehetőségeit, a biztonsági szféra és az informatikai kutatók és fejlesztők közötti együttműködés lehetőségeit az emberi jogok tiszteletben tartásából fakadó kötelezettségeik szigorú szem előtt tartása mellett.

Az „információk" köré csoportosuló, korszerű technológiai környezet adta lehetőségek napjainkban már nélkülözhetetlen „eszközként" segíthetik a biztonságért felelős szervek munkáját. Szerepük felértékelődik a döntéseket megalapozó információk megszerzésének, elemzésének és értékelésének különböző területein. Mind a biztonsági, mind a szűkebben értelmezett nemzetbiztonsági ágazat szereplői számára a nyíltan elérhető digitális adatok és információk olyan fejlődési iránnyá váltak, amelyek mentén az OSINT, a SOCMINT vagy akár Crowdsourcing Intelligence új megoldásai hatékonyan segíthetik az információszerző tevékenységet.

Felhasznált irodalom:

- A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Európai megközelítés az online félretájékoztatás kezelésére, Európai Bizottság, Brüsszel, 2018.4.26. COM (2018) 236 final.
- BENCSIK Andrea: A tudásmenedzsment emberi oldala; Z-Press Kiadó Kft. Miskolc, 2009.
- CASTELLS, Manuel: A tudás világa; Napvilág Kiadó, Budapest, 2006.

[38] Például: https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=fact-checking

- Digital around the world, https://datareportal.com/global-digital-overview#:~:text=Roughly%204.66%20billion%20people%20around,over%20the%20past%20twelve%20months (Letöltés ideje: 2022. 04. 20.)
- DOBÁK Imre: A dezinformáció – napjaink kiemelt kihívása; Katonai Jogi és Hadi Jogi Szemle, 2022/1. http://epa.oszk.hu/02500/02511/00020/pdf/EPA02511_katonai_jogi_szemle_2022_1_093-124.pdf (Letöltés ideje: 2022. 05. 24.)
- EL HOUDAIGUI, Rachid: Terrorism and new technology; https://gnet-research.org/2021/06/24/terrorism-and-new-technology/ (Letöltés ideje: 2022. 05. 18.)
- ENGELKE, Peter: AI, Society, and Governance: An Introduction, Atlantic Council; 2020. https://www.jstor.org/stable/resrep29327 (Letöltés ideje: 2022. 05. 24.)
- GIOE, David V.: „The More thing Change". HUMINT in the Cyber Age; In: DOVER, Robert – DYLAN, Huw – GOODMAN, Michael S. (eds.): The Palgrave Handbook pf Security, Risk and Intelligence; Palgrave Macmillan, London, 2017.
- GREENWALD Glenn: A Snowden-ügy; HVG Könyvek, 2014. ISBN: 9789633041833
- HOWE, Jeff: The Rise of Crowdsourcing, Wired, Jun 1. 2006, Letöltés helye: https://www.wired.com/2006/06/crowds/ (Letöltés ideje: 2022. 05. 24.)
- https://www.bellingcat.com/news/2022/04/14/russias-kramatorsk-facts-versus-the-evidence/ (Letöltés ideje: 2022. 05. 18.)
- https://datareportal.com/global-digital-overview#:~:text=Roughly%204.66%20billion%20people%20around,over%20the%20past%20twelve%20months (Letöltés ideje: 2022. 04. 20.)
- https://www.britannica.com/biography/Julian-Assange (Letöltés ideje: 2022. 05. 17.)
- JÁVOR Endre: A hír, az adat, az információ és a dokumentáció fogalma, helye, szerepe a döntéshozatalban; Nemzetbiztonsági Szemle, 2017/3. pp. 36-60.
- KENT, Sherman: Strategic Intelligence for American World Policy, Princeton University Press, Princeton, 2015. https://doi.org/10.1515/9781400879151 (Letöltés ideje: 2022. 05. 30.)
- KIS Álmos Péter: A hibrid hadviselés természetrajza, Honvédségi Szemle, 2019/4.
- KRANZ, Garry: Metadata, https://www.techtarget.com/whatis/definition/metadata (Letöltés ideje: 2022. 05. 24.)
- LIBICKI, Martin C. The Convergence of Information Warfare; Strategic Studies Quarterly, 2017/1. pp. 49–65. http://www.jstor.org/stable/26271590. (Letöltés ideje: 2022. 05. 20.)

- LOMBARDI, M. – ROSENBLUM, T. – BURATO, A.: From SOCMINT to Digital Humint: re-frame the use of social media within the Intelligence Cycle; Fondazione de Gasperi, 2015.
- MÁTYÁS Szabolcs: Az elemző-értékelő munka gyakorlati aspektusai; NKE KTI, Budapest, 2020. pp. 7-11.
- PORKOLÁB Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? Hadtudomány, 2015/3-4.
- SNOWDEN, Edward – GREENWALD, Glenn: A Snowden-ügy; HVG Könyvek, 2014. ISBN: 9789633041833
- STOTTLEMYER, Steven A.: HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence; International Journal of Intelligence and CounterIntelligence, 2015/3. pp. 578-589, DOI: 10.1080/08850607.2015.992760
- SZABÓ Hedvig – DOBÁK Imre: Az információs társadalom nemzetbiztonsága; Nemzet és Biztonság, 2021/2. pp. 93-110., doi: 10.32576/nb.2021.2.7
- SZELECZKI Zsolt: A tudás menedzsment koncepciója és háttere; Vezetéstudomány, 1999/12. http://unipub.lib.uni-corvinus.hu/5172/1/VT_1999n12p22.pdf (Letöltés ideje: 2022. 05. 10.)
- VIDA Csaba: A hírszerzési ágak elemző-értékelő megközelítése; Felderítő Szemle, 2016/3. pp. 77-94.
- VIDA Csaba: A hírszerző elemző-értékelő munka alapjai; Felderítő Szemle, 2014/3. szám pp. 90-99.
- VIDA Csaba: A nemzetbiztonsági tevékenység szerepe a társadalomban (Gondolatok arról, hogy miért van szükség nemzetbiztonsági szolgálatokra); Hadtudomány, 2015/E. pp. 221-234.
- WAKEFIELD Jane: Deepfake presidents used in Russia-Ukraine war; BBC News, 2022. 03. 18. https://www.bbc.com/news/technology-60780142 (Letöltés ideje: 2022. 05. 18.)
- SPRING Marianna: Marianna Vyshemirsky: 'My picture was used to spread lies about the war'; BBC News, 2022. 05. 16. https://www.bbc.com/news/topics/cjxv13v27dyt/fake-news, (Letöltés ideje: 2022. 05. 18.)
- SHELDON Michael: Russia's Kramatorsk 'Facts' Versus the Evidence; https://www.bellingcat.com/news/2022/04/14/russias-kramatorsk-facts-versus-the-evidence/ (Letöltés ideje: 2022. 05. 18.)
- https://www.bbc.com/news/technology-60780142 (Letöltés ideje: 2022. 05. 18.)
- https://www.bbc.com/news/topics/cjxv13v27dyt/fake-news (Letöltés ideje: 2022. 05. 18.)

SZAKOS JUDIT

VÉDELMI INNOVÁCIÓS ÖKOSZISZTÉMA-FEJLESZTÉS MAGYARORSZÁGON

Bevezetés

Napjaink globális technológiai folyamatai és a legújabb ipari forradalom már nem csak a gazdasági-társadalmi viszonyok egészét, de az értékteremtés módját is megváltoztatta. A forradalmi technológiákban rejlő lehetőségek kiaknázása, valamint a bennük rejlő egyes fenyegetések nemcsak a civil felhasználásban, hanem a védelmi innovációk kapcsán is egyre hangsúlyosabb szerepet kapnak mind a hazai, mind a nemzetközi szakmai közösségben. Az új technológiák nem csak technológiai innováció szintjén jelennek meg, de ezek a „haditechnikai eszközök alapjaiban változtatják meg a jelenlegi hadviselés szabályait és eljárásrendjét".[1]

Az Észak-atlanti Szerződés Szervezete (NATO) Koherens Végrehajtási Stratégiájában hét technológiai prioritást jelöl ki:

1. a mesterséges intelligencia,
2. az adattudomány és számítástechnika,
3. az autonóm rendszerek,
4. a kvantumtechnológia,
5. a biotechnológia,
6. az embert fejlesztő technológiák, a hiperszonikus technológiák,
7. továbbá az űrtechnológia.

Ezzel összhangban Magyarország Nemzeti Katonai Stratégiája a jövő hadviselésével összefüggésben a következő területeken határozza meg a védelmi ipari kapacitások fejlesztését:

- információs technológia és kibervédelem,
- szimulációs, virtuális és augmentált valóság,
- mesterséges intelligencia,
- kvantum számítástechnika,
- robottechnológia,
- pilóta nélküli repülőeszközök és az azok elleni védelem,
- nem halálos fegyverek,
- energiatárolás és alternatív energiaforrások,
- nanotechnológia, anyagtechnológiák és biotechnológia.

Ezekre a fejlesztésekre a civil szférában is jelentős hangsúly kerül, egy-egy fejlesztés ott a védelmi szférával egy időben, vagy már azt megelőzően megjelenik a gazdasági előnyök megszerzése érdekében.[2]

---

[1] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

[2] Magyarország Nemzeti Katonai Stratégiájáról

A civil innováció és a védelmi innováció összhangjára több olyan nemzetközi példát találhatunk, ahol az ország védelmi ipari képessége és a nemzetközi innovációs rangsorokban való elhelyezkedésük egymást erősítő hatásokkal bír. A védelmi szférának az innovációs siker eléréséhez – a kutatás-fejlesztési (K+F) kapacitások kiépítése mellett - többféle kapcsolódása lehet. Ezért a tanulmány során fontos ezeket a lehetőségeket is felvázolni a két legjellemzőbb – állami szerepvállalást is jól érzékeltető – példát bemutatva, ahol a kooperáció és az ösztönzés érvényesül.
Izrael kapcsán számtalan történelmi, kulturális és geopolitikai tényező együttállását láthatjuk, amelyek innovációs hub-ok kialakulásához vezetnek.[3] Kiemelendő egyrészt a hücpe,[4] vagyis az a sajátos stílus, amely segíti a szférában a sikert, másrészt, hogy *„az ország védelme mellett a katonák szolgálati idejük alatt sok olyan képességet elsajátítanak, amire a későbbiekben szükségük lehet. Ami az állam innovációs potenciáljához hozzájárul, az az, hogy a fiatalok a seregben megtanulnak fegyelmezettek lenni, önállóan döntéseket hozni és ha a szükség úgy kívánja, saját találékonyságukat is kifejleszthetik. Mindemellett van még egy fontos tényező, amelyről nem szabad elfeledkezni: a kapcsolati háló."*[5] Az Amerikai Egyesült Államok kapcsán pedig a Fejlett Védelmi Kutatási Projektek Ügynökségét (DARPA) fontos kiemelni, mely élen jár mind a legújabb technológiák fejlesztésének támogatásában, mind az egyes szektorok közötti szinergiák megteremtésében. A szervezet munkájához köthetjük többek között az internet vagy a GPS megvalósulását.

A NATO kapcsolódó törekvései mellett 2021-től az Európai Unióban is elérhetővé válik a polgári K+F programok mellett az Európai Védelmi Alap (EDF) mind az alacsony, mind a magas technológiai érettségi szintű kutatási és fejlesztési projektekre.[6]
Ezek a projektek – az elérhető források körének bővítése mellett – egyrészt összhangban állnak, másrészt modellként szolgálhatnak a nemzeti védelmi ipar kialakítására tett törekvésekkel hazánkban a megkerülhetetlenné vált technológiai fejlődés kapcsán. A védelmi innovációs ökoszisztéma kiépítésének bázisa a meglévő polgári innovációs és kutatás-fejlesztési környezet.

Módszertan

A tanulmány elméleti keretét a nem-lineáris innovációs modellek adják, a modellek irányából tekint a védelmi innovációkra az innovációs ökoszisztémán belül. A modellekből az állami szerepvállalást kiemelve megvizsgálja Magyarország potenciális kitörési lehetőségeinek szinergiáját. A kutatás mind a védelmi innovációs ökoszisztéma hazai szakirodalmára, mind az innovációs ökoszisztémákat leíró

[3] SENOR, Dan – SINGER, Saul: Startra kész nemzet - Izrael gazdasági csodájának története; Patmos Records, 2012.

[4] *„[A] hücpe, vagyis az izraeliek sajátos magatartása. Ebben a közvetlen stílusban benne van minden, ami az innovációhoz szükséges. A hücpe jelenti azt, hogy a munkavállalók megkérdőjelezik a munkaadókat és azt is, hogy a közalkalmazottak kijavítják a „felsőbbrendű" minisztereket."* Lásd: BALOGH Bettina: Izrael innovációs potenciáljának alappillérei; Iskolakultúra, 2016/12. pp. 65-75.

[5] Uo. p. 71.

[6] 1456/2021. (VII. 13.) Korm. határozat Magyarország Kutatási, Fejlesztési és Innovációs stratégiájának (2021–2030) elfogadásáról

nemzetközi modellekre épít, kiegészítve egyéb releváns forrásokkal. A téma jellegéből adódóan az állami törekvések vizsgálata a nyilvánosan elérhető stratégiai dokumentumokon és tájékoztatókon.[7]

Az innovációs ökoszisztémát leíró modellek

Az innováció fogalma és az ezt keretező modellek az évek során jelentős fejlődésen mentek keresztül. A termékek fejlesztésétől eljutottunk az Oslo Kézikönyv 2018-as definíciójáig, amely szerint *„az innováció új, vagy jelentősen javított termék vagy eljárás, vagy ezek kombinációja, mely jelentősen különbözik a szereplő korábbi termékeitől, illetve eljárásaitól és elérhető a vásárlók részére (termék) vagy használatba vették (eljárás).”*[8] Ez már magába foglalja a nem-technológiai innovációkat is. Fontos rendezési szempont a radikális és az inkrementális (fejlesztő) innovációk megkülönböztetése is.[9]

Az innováció létrejöttét vizsgáló modellek előbb az ötlet, illetve a kutatás-fejlesztési folyamat és a piac közötti lineáris út leírásán dolgoztak,[10] majd eljutottak a rendszerszintű vizsgálatig, bevonták a vizsgálatba a nem-technológiai innovációkat és a rendszer valamennyi szereplőjét (organizations), továbbá az – intézményi közgazdaságtani értelemben vett – „intézményeket” (institutions/rules) is elkezdték figyelembe venni.[11] Utóbbiak lehetnek formális szabályok vagy informális szokások is.

A nem-lineáris innovációs modellek közül a *Triple Helix Modell* az innováció létrejöttét már nem egy légüres térben működő gyár önálló teljesítményének tekinti, hanem leírja, hogy több szereplő eredményes együttműködése egy innovációt elősegítő környezetet képes létrehozni. A modell – a vizsgált szektortól függetlenül – a releváns aktorokat is megnevezi, akik együttműködése az innováció sikeréhez nélkülözhetetlen. Ezek:

- ezek az állam,
- az egyetemek,
- az ipar közötti kapcsolódások.

Megjelenik a szereplők közötti tudástranszfer, interakció és egymás folyamatos fejlődésre ösztönzése, egymás szerepeinek átvétele mellérendelt pozícióban. Megfigyelhető, hogy az egyensúlyi állapotból való kimozdulás – akár az interakciók

---

7 A stratégiák feldolgozása a MAXQDA szövegelemző szoftver segítségével történt.

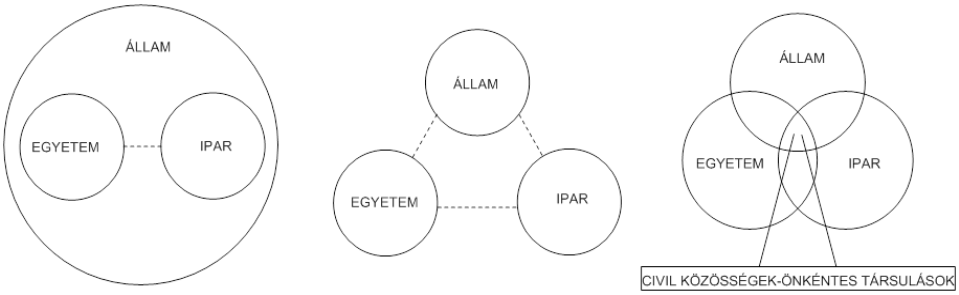
8 OECD: Oslo Manual 2018 – Guidelines for Collecting, Reporting and Using Data on Innovation. 4. kiadás. 2018. Online: https://www.oecd.org/science/oslo-manual-2018-9789264304604-en.htm. (Letöltés ideje: 2020. 05. 26.)

9 MAKÓ Csaba – ILLÉSSY Miklós – HEIDRICH Balázs: When will alpha and omega collide? In search of the theoretical relevance of EU innovation policies; Vezetéstudomány - Budapest Management Review, 2019/11. pp. 67-68. Online: https://doi.org/10.14267/VEZTUD.2019.11.05.

10 A lineáris innovációs modellek típusai: a szükségletteremtő, a szükségletkövető és az interaktív modell. Lásd: DORA, Marinova – PHILLIMORE, John: Models of Innovation; The International Handbook on Innovation, Oxford, Pergamon, 2003. pp. 44-53. Online: https://doi.org/10.1016/B978-008044198-6/50005-X.

11 MAKÓ Csaba – ILLÉSI Miklós – SZÁMADÓ Róza – SZAKOS Judit: Workplace innovation: Concepts, regulation and increasing role of knowledge management: Theoretical considerations and European experiences; Pro Publico Bono–Public Administration; 2020/1. pp. 96-123.

tompulása, akár az egyenrangú partnerség felbomlása valamelyik szereplő javára – a hatékonyság ellen hat.[12]



1. ábra: A Triple Helix Modell megjelenési formái. Az innovációt rendszerszinten az együttműködő, jobb oldali forma ösztönzi[13]

Az 1. ábra a modell három tipizált megjelenési formáját tartalmazza, ahol az első a versenytorzító állami dominanciát, a második az ún. laissez-faire altípust,[14] vagyis az aktorok erős különválasztását, míg a harmadik a visszacsatolásokkal erősített, innovációt leginkább ösztönző formát jeleníti meg. Az interakció a három szféra keresztmetszetében lévő hibrid intézményeken keresztül valósul meg.[15]

A *Triple Helix Modell kiterjesztett változatai* bevonják a vizsgálatba a média- és kultúra alapú társadalom, illetve a természeti-környezeti tényezőket is.[16] Utóbbi,

---

12 ETZKOWITZ, Henry: The Triple Helix: University – Industry – Government Innovation in Action; New York, Routledge Taylor & Francis Group, 2008. pp. 1-8. Online: https://doi.org/10.4324/9780203929605.

13 Forrás: Uo. pp. 12-16. alapján saját szerkesztés

14 Ugyanakkor meg kell jegyezni, hogy bár a legtöbb megközelítés az amerikai példát pont a távolságtartó kategóriába sorolja, ez az elválasztás az említett DARPA, illetve a Nemzeti Repülési és Űrhajózási Hivatal (NASA) esetében vitatható Mazzucato vállalkozó állam koncepciója mentén.
CHOI, Joonhwan– LEE, Jaegul: Repairing the R&D Market Failure: Public R&D Subsidy and the Composition of Private R&D.; Research Policy, 2017/8. pp. 1465–1478. Online: DOI: 10.1016/j.respol.2017.06.009
Mariana Mazzucato: *Mission-Oriented Research & Innovation in the European Union. A problem-solving approach to fuel innovation-led growth*. Luxemburg, European Commission, 2018.
MAZZUCATO, Mariana – ROBINSON, Douglas K. R.: Co-Creating and Directing Innovation Ecosystems? NASA's Changing Approach to Public-Private Partnerships in Low-Earth Orbit; Technological Forecasting and Social Change, 2018/136. pp. 166-177. Online: https://doi.org/10.1016/j.techfore.2017.03.034.

15 VAS Zsófia Boglárka: Tudásalapú gazdaság és társadalom kiteljesedése: A Triple Helix továbbgondolása – a Quadruple és Quintuple Helix. Dialógus a regionális tudományról; Győr, Széchenyi István Egyetem Regionális- és Gazdaságtudományi Doktori Iskola, 2012. pp. 198-206.

16 A jelen tanulmányban említett kiterjesztett helix modellek: a Quadruple Helix Modell és a Quintuple Helix Modell. Ez a szemlélet már bevonja a vizsgálatba a tudásalapú gazdaság, tudásalapú társadalom és tudásalapú demokrácia fogalmakat.
CARAYANNIS, Elias G. – BARTH, Thorsten D.– CAMPBELL, David F.J: The Quintuple Helix Innovation Model: Global Warming as a Challenge and Driver for Innovation; Journal of

földrajzi elhelyezkedésre alapuló megközelítés Izrael innovációs ökoszisztémájának példájánál különösen szemléletes.[17]
A Massachusetts Institute of Technology (MIT) 5 dimenziós modellje a kockázati tőke, a nagyvállalatok, a kormányzat, az egyetemek és a vállalkozók hálózatával írja le a rendszert.[18]
A keretek kialakítása (intézmények) és a kiemelt szervezetek mellett azonban a szektor és a földrajzi egység igényeinek megfelelő további aktorokat is azonosíthatunk, továbbá nem elhanyagolható az infrastruktúra szerepe sem.

A védelmi innovációs ökoszisztéma

„A hadsereg szigorúan szervezett erős fegyelemmel rendelkező szervezet, amelyben dominál a rendfokozati hierarchia, a szigorú alá- és fölérendeltségi viszony. Ilyen értelemben a weberi bürokráciának egy extrém megnyilvánulási formája, amely egyrészt magas fokú szervezettséggel rendelkezik, másrészt rugalmatlan is, mert nem bátorítja a kezdeményezőkészséget és az innovációt."[19] Ugyanakkor, ahogy elméletben a kiterjesztett Triple Helix Modell is ábrázolja, gyakorlati eseteket keresve az izraeli példában a hüpce, az Egyesült Államokban a vállalkozó szemlélet és a kudarctűrés kultúrája mutatja, más mód is létezik, ha az innovatív készséget állítjuk a középpontba a védelmi innováció ösztönzése során. Az innovációt és kooperációkat támogató szemléletmód (mindset) és a képességfejlesztés megjelenése ösztönözni tudja az innovációt az ökoszisztémát kiépíteni készülő területi régiókban is. A hadsereg ugyanis számos – az élet valamennyi területén változást indukáló – újítást tud kezdeményezni, finanszírozni és megvalósítani. Példaként említhető, amikor az Amerikai Védelmi Minisztérium az 1960-as években egy decentralizált postai szolgáltatás kialakítását tűzte ki célul, hogy a központ esetleges lerombolása esetén ne omoljon össze a hagyományos levelezőrendszer. Az általuk finanszírozott kutatás az email megszületéséhez vezetett, ezzel pedig valóban sikeresen decentralizálták a kommunikációt egy innovációval.[20]
Ma a stratégiai versenyelőnyhöz már nem csak *„a gépi rendszerek, az automatika, az elektronika és az informatika, illetve a hírközlés szerepe (…) erős túlsúlyba kerülését fontos prioritásként kezelni, de azt is, hogy „mennyi idő alatt fut le egy haditechnikai kutatás-fejlesztési projekt, illetve az új termékek rendszeresítése és alkalmazásba vétele, mint ciklus."*[21]

Innovation and Entrepreneurship, 2012/1. pp. 1-12. Online: https://doi.org/10.1186/2192-5372-1-2

17 SENOR – SINGER i.m.

18 Ezt a modellt eredetileg a kiberbiztonsági innovációs ökoszisztéma leírására hozták létre. Lásd: MURRAY, Fiona– BUDDEN, Phil: MIT's Stakeholder Framework for Building & Accelerating Innovation Ecosystems; Working Paper, MIT's Laboratory for Innovation Science & Policy, 2019.

19 SZENES Zoltán: A védelempolitika fogalma, tartalma és határai; Nemzet és Biztonság, 2008/2. pp. 27-34.

20 KORNAI János: Innováció és dinamizmus: Kölcsönhatás a rendszerek és a technikai haladás között; Közgazdasági Szemle, 2010/2.
Hiába beszélhetünk azonban egy mindennapokban is használt eszközről, a kezdeményezés és finanszírozás miatt nem a hagyományos (schumpeteri) innovációk közé tartozik az online levelezés kifejlesztése.

21 PORKOLÁB Imre – HENNEL Sándor – HEGEDŰS Ernő: Az innováció fókuszú digitális fejlesztésen alapuló stratégia; Hadtudomány, 2021/3. pp. 11-22.

A NATO is deklarálta, hogy *„[a] technológiai változások sebessége soha nem volt még ilyen gyors, ami új lehetőségeket és kockázatokat teremt a biztonsági környezetben és a NATO működésében”*.[22] Ezért kiemelt figyelmet fordítanak a feltörekvő, illetve forradalmi technológiák azonosítására, kifejlesztésére és alkalmazására, amelyben segítséget tud biztosítani a 2021. júniusban felállított Észak-atlanti Védelmi Innovációs Akcelerátor (DIANA, Defence Innovation Accelerator for the North Atlantic) és a NATO Innovációs Alap (NATO Innovation Fund), melyek szervezeti támogatást tudnak biztosítani azoknak a startupoknak, amik kettős felhasználású technológiák kidolgozásában vesznek részt.[23]

Hazánkban az elmúlt huszonöt év legnagyobb és legátfogóbb honvédelmi programjaként a Honvédelmi és Haderőfejlesztési Program[24] – a nemzetközi folyamatokkal összhangban – számos modernizációhoz és innovációhoz kapcsolható tényezőt deklarál. A védelmi célú kutatás-fejlesztési és innovációs ökoszisztéma kialakítása mellett a hazai védelmiipar fejlesztése szerepel a célkitűzések között. *„A program elődleges célja egy korszerű eszközökkel felszerelt, a kor biztonsági kihívásaira adekvát válaszokat adó honvédség létrehozása úgy, hogy biztosítva legyen a társadalomból építkező hátország is, amely önként, de tudatosan gondolkodik és tesz az ország biztonságáért.”*[25]
A célrendszerről és az előrehaladásról részletesen Dr. Palkovics László innovációs és technológiai miniszter 2021. június 8-án számolt be az Országgyűlés Honvédelmi és Rendészeti bizottságának. Tájékoztatása szerint a védelmi ipar jelentősége a járműiparéval vetekszik, és Magyarországon *„a high-tech iparágak közül az elsők között szerepel”*. A hazai ipari kultúra (például járműipar, gépipar, elektronikai ipar) megfelelő alapjai lehetnek hadiipari eszközök fejlesztésének, gyártásának és értékesítésének. A fejlesztési céloknál azonban célirányos kutatásra van szükség, a stratégia céljaival *„a DARPA működését próbáltuk a magyar viszonyok között megjeleníteni”*, illetve felismeri a többi – megnevezve a civil – szektor megoldásainak érdekességét minőségi és költséghatékonysági szempontból.[26] Ez a két állítás párhuzamba állítható a vállalkozó állam koncepció küldetésorientált felfogásával, ahol a fejlesztési irányoknak, vagyis a *„küldetésnek elég tágnak kell lennie ahhoz, hogy különböző szektorokat ösztönözzön (az ember Holdra szállása is tucatnyi ágazat együttműködését igényelte), de elég konkrétnak is kell lennie ahhoz, hogy azt különböző megoldható problémákra lehessen bontani, így a küldetés folyamata rendszeresen ellenőrizhetővé váljon.”*[27]
Az azonosított kockázati területek és fókuszpontok: a felsőoktatás és a szakképzés (a Triple Helix és az MIT Modellben is azonosított terület); a hazai beszállítói kör

---

[22] PORKOLÁB Imre – HŐNICH Artúr: A NATO útja a DIANA létrehozásáig és főbb fókuszterületei a védelmi innováció keretében; Honvédségi Szemle 2021/6. pp. 20-35.
[23] PORKOLÁB– HÖNICH i.m.
[24] A stratégiáról részletesen lásd: BUDAVÁRI Krisztina: A Zrínyi 2026 program. Korlátozott lehetőségek a magyar védelmi ipar fejlesztésére; Hadtudomány 2019/3. pp. 142-159. Online: DOI 10.17047/HADTUD.2019.29.3.142
[25] Magyarország Kutatási, Fejlesztési és Innovációs Stratégiája
[26] DR. PALKOVICS László: Tájékoztató a védelmi ipar helyzetéről; Országgyűlés Honvédelmi és rendészeti bizottság, 2021. 06. 08. Online: https://www.parlament.hu/documents/static/biz41/bizjkv41/HOB/2106081.pdf (Letöltés ideje: 2022. 01. 31.)
[27] MAZZUCATO, Mariana: From Market Fixing to Market-Creating: A New Framework for Innovation Policy; Industry and Innovation, 2016/2. pp. 140-156. Online: https://doi.org/10.1080/13662716.2016.1146124.

kapacitásai és méretspecifikus kérdések. Előremutató cél Magyarország pozícionálása a tudásintenzív területeken, ahol megjelenik az innováció és a kutatás-fejlesztés. A hibrid, klaszterekben történő fejlesztés pedig nem csak védelmi ipari, hanem gazdaságfejlesztési célokat is kitűz. A megnevezett hálózatokban megjelennek a horizontális együttműködések (oktatás különböző szintjei, kutatás, gyártás).[28] A gazdasági hasznosulás lehetőségeire reflektál, hogy Magyarország újraiparosítási stratégiája, az Irinyi terv is a támogatandó iparágak közé emelte a védelmi ipart. Az Intelligens Szakosodás Stratégia[29] pioritásként kezeli és a védelmi ipar részének tekinti a kettős felhasználású élvonalbeli technológiai termékek és szolgáltatások gyártását, illetve az előállításukra szolgáló innováció támogatását. Deklarálja továbbá, hogy *„[a] XXI. századra fokozottan jellemző digitalizáció és robotizáció korában a kiber- és egyéb biztonsági kihívásokra tekintettel, az S3-hoz kapcsolódóan megvalósított fejlesztések során a hazai szellemi tulajdon védelmi, adatvédelmi és nemzetbiztonsági követelményeket, illetve a nemzeti ellenállóképesség és a (védelmi ipar esetén) a kettős hasznosíthatóság egységes szempontjait az érintetteknek maradéktalanul érvényre kell juttatni”* ágazati klaszterrendszer kiépítésével.
Az újrastrukturálás lehetőséget adhat együttműködésre az egyetemi és kutatóintézeti partnerekkel, de kiléphet a pusztán akadémiai kapcsolatépítésből és az innovációs ökoszisztéma felé is keresheti az együttműködési lehetőségeket, így az innovációs központok, nagy növekedési potenciállal rendelkező startup vállalatok, kis- és középvállalatok, ipari szereplők is a fókuszba kerülhetnek.[30] Hasonló kezdeményezés már látható volt a HM Modernizációs Intézetnél a NATO Innovációs Kihívás kapcsán, ahol kapcsolódó magyar startup cégek mentorálására is sor került.[31] A hazai startup ökoszisztémával való együttműködésben általánosan is potenciális kapcsolódások vannak a védelmi innováció terén.[32] Az innovációs ökoszisztéma és a védelmi innovációs ökoszisztéma kapcsolatának potenciálja rajzolható ki a hazai tendenciákból is.

A Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet szabályozza a védelmi innovációhoz és védelmi ipar fejlesztéséhez kapcsolódó hatásköröket. Az új kormányzati struktúrában a Honvédelmi Minisztérium felel a védelmi innováció és védelmi iparfejlesztés stratégiai irányainak meghatározásáért, a Technológiai és Ipari Miniszter az iparügyekért való felelőssége keretében – a védelmi fejlesztésekért felelős miniszterrel együttműködve – végrehajtja a védelmi ipari beruházások megvalósításával kapcsolatos feladatokat és működteti a védelmi ipari feladatok végrehajtásának rendszerét.
Az Állam annak érdekében, hogy reflektálni tudjon napjaink kihívására, létrehozott több, innovációért felelős intézményt, illetve társaságot: a Honvédelmi Minisztérium

---

28 PALKOVICS i.m.

29 1428/2021. (VII. 2.) Korm. határozat a 2021–2027. évekre vonatkozó Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról

30 Dr. BENKŐ Tibor vezérezredes, honvédelmi miniszter előadása a Hogyan tovább Magyarország? Védelem és Biztonság című konferenciáján. 2019. 05. 22. és PORKOLÁB – HÖNICH i.m. alapján.

31 HEGEDŰS Ernő – SZIVÁK Petra: NATO Védelmi Innovációs Nap. Tudósítás az MH Modernizációs Intézet nemzetközi rendezvényéről. Haditechnika, 2020/1. pp. 48-53. Online: DOI: 10.23713/HT.54.1.10

32 PORKOLÁB Imre: Védelmi innováció és katonai képességfejlesztés; Magyarország 2020. 50 tanulmány az elmúlt 10 évről. MCC, 2021. pp. 779-798.

Modernizációs Intézetét, a Transzformációs Parancsnokságot, vagy a Védelmi Innovációs Kutatóintézet Közhasznú Nonprofit Zrt-t.[33]

Következtetések: a technológiai innováción túl

A programokban és stratégiákban előrevetített technológiai fejlesztések és a védelmi ipar kiépítése az elméleti részben bemutatott innovációs aspektusok mentén valósul meg. Ezzel együtt Magyarország Nemzeti Katonai Stratégiája szerint *„[a] Magyar Honvédségnek a kor követelményeinek megfelelő, szemléletében, szervezeti kultúráját és haditechnikáját tekintve is megújult, jól szervezett, a nemzeti hagyományokat tiszteletben tartó és ápoló, önállóan, szövetségi és európai uniós keretek között is hatékonyan alkalmazható, képességeit tartalékos rendszerrel megerősítő, fenntartható haderővé kell válnia. Hazai és nemzetközi feladatai végrehajtása érdekében korszerűen felszerelt és kiképzett katonákkal, valamint rugalmasan alkalmazkodni képes, hatékonyan alkalmazható, telepíthető és fenntartható katonai képességekkel kell rendelkeznie.” „A műveleti környezeti változásokhoz történő hatékony alkalmazkodás érdekében létrejön a Magyar Honvédség kutatás-fejlesztési és innovációs ökoszisztémája, és folytatódik transzformációs rendszerének fejlesztése. Ehhez egységes rendszerbe szükséges foglalni a Magyar Honvédség kutatás-fejlesztési, innovációs, koncepció- és doktrínafejlesztési, valamint felkészítési és kiképzési rendszerét.”*

A rendszermodelleknél említett tudásmegosztás, tudástranszfer, informális szokások, normák kialakítása mellett visszatérő motívum a bizalom és egymás megismerésének, kapcsolatok kiépítésének kérdése. Az igénytől a rendszeresítésig tartó ciklusidők rövidülése miatt jelentősen lecsökken a szervezeti intézményi alkalmazkodási időszak, ez a tanulási folyamatok radikális reformjához vezet,[34] valamint felértékeli a szervezeti és eljárásinnovációk szerepét. A fejlesztés során ezek szintén olyan aspektusok, amik másolhatatlanok, ugyanakkor a tanulási folyamat sokat segíthet ezeknek az ún. „soft” aspektusoknak a kialakításához. Itt tér vissza a korábban említett mindset és kapcsolatrendszer – mint informális együttműködés – jelentősége is.

Nagy hangsúly helyeződik továbbá a formális együttműködésekre. A tanulmányban bemutatott törekvésekből az innovációs modellek valamennyi aspektusa világosan kitűnik: az alapozó fizikai infrastruktúra építéstől – legalább, de nem kizárólagosan – az oktatás (valamennyi szintje), a kutatóhelyek, a kis- és közepes, illetve a multinacionális vállalatok, a kockázati tőkebefektetők és az állam képviseletében megjelenő szereplők kapcsolódása mind megfigyelhetőek, valamint a releváns startup vállalatokkal való együttműködésre is vannak törekvések. A gazdasági és akadémiai szereplők mellett azonban megjelenik a kooperációs igény – a haderőépítés moduláris építőköveként – a „rendőri erőkkel, civil hatóságokkal, társadalmi szervezetekkel és nemzetközi intézményekkel”,[35] amely később további formális és informális hálózatokat jelenthet.

---

[33] PORKOLÁB–HÖNICH i.m.

[34] PORKOLÁB–HENNEL–HEGEDŰS i.m.

[35] SZENES Zoltán: Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek; Biztonsági kihívások a 21. században, Budapest, Dialóg Campus, 2017. pp. 69-104.

A Triple Helix Modell és az MIT 5 dimenziós modelljének valamennyi aspektusát beépítik az állami stratégiákba és programokba. A védelmi innovációs ökoszisztéma kiépítésével felfedezhető a misszióvezérelt, vállalkozó állam-koncepció, amely azonban nem zárja ki a célvezérelt kutatások átvándorolását a civil szférába, és megjelenésüket a piacon. Ezek a kutatások pedig összhangban tudnak lenni a modern kor kihívásaival, hozzájárulva a tudásalapú társadalom kiépítéséhez, és a fenntartani kívánt biztonsághoz.

Felhasznált irodalom:

- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
- 1428/2021. (VII. 2.) Korm. határozat a 2021-2027. évekre vonatkozó Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról
- 1456/2021. (VII. 13.) Korm. határozat Magyarország Kutatási, Fejlesztési és Innovációs stratégiájának (2021-2030) elfogadásáról
- BALOGH Bettina: Izrael innovációs potenciáljának alappillérei; Iskolakultúra, 2016/12. pp. 65-75.
- BUDAVÁRI Krisztina: A Zrínyi 2026 program. Korlátozott lehetőségek a magyar védelmi ipar fejlesztésére; Hadtudomány 2019/3. pp. 142-159. Online: DOI 10.17047/HADTUD.2019.29.3.142
- CARAYANNIS, Elias G. – BARTH, Thorsten D. – CAMPBELL, David F.J: The Quintuple Helix Innovation Model: Global Warming as a Challenge and Driver for Innovation; Journal of Innovation and Entrepreneurship, 2012/1. pp. 1-12. Online: https://doi.org/10.1186/2192-5372-1-2
- CHOI, Joonhwan– LEE, Jaegul: Repairing the R&D Market Failure: Public R&D Subsidy and the Composition of Private R&D.; Research Policy, 2017/8. pp. 1465-1478. Online: DOI: 10.1016/j.respol.2017.06.009
- DORA, Marinova – PHILLIMORE, John: Models of Innovation; The International Handbook on Innovation, Oxford, Pergamon, 2003. pp. 44-53. Online: https://doi.org/10.1016/B978-008044198-6/50005-X.
- Dr. Benkő Tibor vezérezredes, honvédelmi miniszter előadása a Hogyan tovább Magyarország? Védelem és Biztonság című konferenciáján. 2019. 05. 22.
- DR. PALKOVICS László: Tájékoztató a védelmi ipar helyzetéről; Országgyűlés Honvédelmi és rendészeti bizottság, 2021. 06. 08. Online: https://www.parlament.hu/documents/static/biz41/bizjkv41/HOB/2106081.pdf (Letöltés ideje: 2022. 01. 31.)
- ETZKOWITZ, Henry: The Triple Helix: University – Industry – Government Innovation in Action; New York, Routledge Taylor & Francis Group, 2008. Online: https://doi.org/10.4324/9780203929605.

- HEGEDŰS Ernő – SZIVÁK Petra: NATO Védelmi Innovációs Nap. Tudósítás az MH Modernizációs Intézet nemzetközi rendezvényéről. Haditechnika, 2020/1. pp. 48-53. Online: DOI: 10.23713/HT.54.1.10
- KORNAI János: Innováció és dinamizmus: Kölcsönhatás a rendszerek és a technikai haladás között; Közgazdasági Szemle, 2010/2.
- MAKÓ Csaba – ILLÉSI Miklós – SZÁMADÓ Róza – SZAKOS Judit: Workplace innovation: Concepts, regulation and increasing role of knowledge management: Theoretical considerations and European experiences; Pro Publico Bono–Public Administration; 2020/1. pp. 96-123.
- MAKÓ Csaba – ILLÉSSY Miklós – HEIDRICH Balázs: When will alpha and omega collide? In search of the theoretical relevance of EU innovation policies; Vezetéstudomány - Budapest Management Review, 2019/11. pp. 66-73. Online: https://doi.org/10.14267/VEZTUD.2019.11.05.
- MAZZUCATO, Mariana – ROBINSON, Douglas K. R.: Co-Creating and Directing Innovation Ecosystems? NASA's Changing Approach to Public-Private Partnerships in Low-Earth Orbit; Technological Forecasting and Social Change, 2018/136. pp. 166-177. Online: https://doi.org/10.1016/j.techfore.2017.03.034.
- MAZZUCATO, Mariana: From Market Fixing to Market-Creating: A New Framework for Innovation Policy; Industry and Innovation, 2016/2. pp. 140-156. Online: https://doi.org/10.1080/13662716.2016.1146124.
- MAZZUCATO, Mariana: Mission-Oriented Research & Innovation in the European Union. A problem-solving approach to fuel innovation-led growth; European Commission, Luxemburg, 2018. Online: https://ec.europa.eu/info/sites/default/files/mazzucato_report_2018.pdf (Letöltés ideje: 2022. 01. 31.)
- MURRAY, Fiona– BUDDEN, Phil: MIT's Stakeholder Framework for Building & Accelerating Innovation Ecosystems; Working Paper, MIT's Laboratory for Innovation Science & Policy, 2019.
- OECD: Oslo Manual 2018 – Guidelines for Collecting, Reporting and Using Data on Innovation. 4. kiadás. 2018. Online: https://www.oecd.org/science/oslo-manual-2018-9789264304604-en.htm. (Letöltés ideje: 2020. 05. 26.)
- PORKOLÁB Imre – HENNEL Sándor – HEGEDŰS Ernő: Az innováció fókuszú digitális fejlesztésen alapuló stratégia; Hadtudomány, 2021/3. pp. 11-22.
- PORKOLÁB Imre – HŐNICH Artúr: A NATO útja a DIANA létrehozásáig és főbb fókuszterületei a védelmi innováció keretében; Honvédségi Szemle 2021/6. pp. 20-35.
- PORKOLÁB Imre: Védelmi innováció és katonai képességfejlesztés; Magyarország 2020. 50 tanulmány az elmúlt 10 évről. MCC, 2021. pp. 779-798.
- SENOR, Dan – SINGER, Saul: Startra kész nemzet - Izrael gazdasági csodájának története; Patmos Records, 2012.
- SZENES Zoltán: A védelempolitika fogalma, tartalma és határai; Nemzet és Biztonság, 2008/2. pp. 27-34.

- SZENES Zoltán: Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek; Biztonsági kihívások a 21. században, Budapest, Dialóg Campus, 2017. pp. 69-104.
- VAS Zsófia Boglárka: Tudásalapú gazdaság és társadalom kiteljesedése: A Triple Helix továbbgondolása – a Quadruple és Quintuple Helix. Dialógus a regionális tudományról; Győr, Széchenyi István Egyetem Regionális- és Gazdaságtudományi Doktori Iskola, 2012. pp. 198-206.

E SZÁMUNK TARTALMA

CONTENTS

CSABA VIDA DR.

THE ROLE OF SOCMINT IN THE INTELLIGENCE ANALYSIS
INTELLIGENCE ANALYSIS APPROACH OF THE NEW INTELLIGENCE DISCIPLINE

The author examines the newest intelligence discipline, that is Social media intelligence (SOCMINT) in his study. He shows the formation of the SOCMINT, and its role and place of the activity of the intelligence and counter intelligence. He reviews the fields of SOCMINT, that are social media/networks for the purpose of what information can be gathered. He analyses the specificity of SOCMINT information, mainly in terms of intelligence. He defines the conceptual scope of SOCMINT as well as the characteristics of intelligence disciplines, taking into account the international literature. He divided the process of SOCMINT into four phases, these are: the searching data gathering capabilities, information gathering, data processing and dissemination to the intelligence analysts. In the second half of the study, he explains the relationship between the SOCMINT and others intelligence disciplines, after that analyse its contact with the intelligence analysis.

Keywords: intelligence, counter intelligence, SOCMINT, intelligence analysis

SÁNDOR BABOS

A SOCIAL SCIENCE APPROACH TO NATIONAL SECURITY ACTIVITY

Nowadays, the activities of national security, including intelligence services, such as intelligence and countermeasures, are mostly examined from the point of view of legal and content, the authority given to them, the appropriate system of tools and methods, or historical, ie case studies. Nevertheless, the services themselves are an integral part of society and the staff of the secret services are an integral part of society. For all these reasons, in addition to the usual legal or, in some cases, historical approach, it is worthwhile to conduct research in the fields of political science, sociology, psychology, philosophy and pedagogy, as well as economics. Most of the social sciences listed have already produced works that can provide a starting point for this, and a comprehensive study is yet to come.
The present study attempts to delineate the social science research directions of the national security activity and the secret services, and makes suggestions for the necessary further research.

Keywords: national security, social science, political science, psychology, sociology

SUHAJDA ATTILA – DR. RITECZ GYÖRGY

A TERRORIZMUS ÉS A MIGRÁCIÓ (MENEKÜLTEK) KÖZÖTTI KAPCSOLAT ELEMZÉSE

A tanulmány napjaink két fontos társadalmi jelenségének, a migrációnak és a terrorizmusnak kapcsolatát kívánja vizsgálni globális szinten, a kétpólusú világrend összeomlásától napjainkig, és kísérletet tesz az egyes trendfordulók meghatározására és a mögöttes okok feltárására. A tanulmány bemutatja a migráció és a terrorizmus közötti ok-okozati viszonyt, legalábbis ami a hivatalos statisztikai adatok alapján feltárható, valamint ezek kapcsolódását a szélsőséges ideológiához. Az elemzés három mutató (terrorcselekmények száma, a menekültstátuszt kapott személyek száma, és a több adatból összevont menekülők száma) elemzésével próbálja megválaszolni a migráció és a terrorizmus közötti összefüggés jellegét.

***Kulcsszavak*:** migráció, terrorizmus, szélsőséges ideológiák, kauzalitás, elemzés

TÓTH TAMÁS

MAGYARORSZÁG NEMZETI BIZTONSÁGI STRATÉGIAI EVOLÚCIÓJA, ANNAK AKTUALITÁSAI ÉS FŐBB NEMZETBIZTONSÁGI VETÜLETEI

A 21. századra látható vált, hogy korunk biztonságot veszélyeztető külső tényezői rendkívül dinamikusan, sokszor csak korlátozottan előrejelezhető módon változnak, gondoljunk csak a 2022-es fegyveres orosz-ukrán konfliktusra, és annak nem várt gazdasági, humanitárius és társadalmi hatásaira. A változások megfelelő lereagálásához szükséges védendő érdekek, célok, intézkedések meghatározása folyamatos harmonizációt követelnek az államok átfogó biztonsági stratégiai dokumentumai tekintetében is, amelyek végrehajtásában hazai viszonylatban is egyre fokozottabb szerep jut a nemzetbiztonsági ágazat szereplőinek. Jelen publikáció fő célja a hazai biztonsági és védelmi tárgyú átfogó stratégiák evolúciójának áttekintése, és az evolúciós folyamatok nemzetbiztonsági szervezetrendszerre gyakorolt hatásainak vizsgálata.

Kulcsszavak: nemzeti biztonsági stratégia, nemzetbiztonság, biztonsági környezet, biztonsági kihívás

ATTILA SUHAJDA – GYÖRGY RITECZ DR.

ANALYSIS OF THE RELATIONSHIP BETWEEN TERRORISM AND MIGRATION (REFUGEES)

The study examines the connection between terrorism and migration on a global level, from the collapse of the bipolar world order. The study makes an attempt to identify trend-turning points, and to explore their reasons in the background. The study presents those connecting points existing between migration and social integration that are relevant in the case of various radical ideologies and terrorism. The analysis intends to provide answers for the nexus between migration and terrorism with the help of three indicators (number of terror attack, number of person with refuge status, number of flying people it's an indicator with the fusion of many data).

***Keywords*:** migration, terrorism, radical ideologies, casuality, analysis

TAMÁS TÓTH

HUNGARY'S NATIONAL SECURITY STRATEGIC EVOLUTION, ITS ACTUALITIES AND MAIN NATIONAL SECURITY ASPECTS

By the 21st century, it has become clear that the external factors threatening the security of our time are changing very dynamically, often with limited predictability, just think of the 2022 armed Russian-Ukrainian conflict and its unexpected economic, humanitarian and social consequences. The definition of the interests, goals and measures to be protected necessary for the proper response to the changes also requires continuous harmonization with regard to the comprehensive security strategic documents of the states, in the implementation of which the actors of the national security sector play an increasingly important role. The main goal of this publication is to review the evolution of comprehensive security and defense strategies in Hungary and to examine the effects of evolutionary processes on the national security organization system.

Keywords: national security strategy, national security, security environment, security challenge

NEUSPILLER FERENC

A NATO „LEGGYENGÉBB LÁNCSZEME”? OLASZORSZÁG KATONAPOLITIKAI HELYZETE 1963-1975.

A második világháború után Olaszország a nyugati tömb oldalán kötelezte el magát. Bár a hidegháborúban az 1960-as és az 1970-es éveket az enyhülés jellemezte, a két szemben álló katonai szövetség és a két szuperhatalom között továbbra is voltak konfliktusok. Olaszország a NATO egyik alapítótagjaként fontos szerepet játszott a Földközi-tenger és a Szövetség déli szárnyának védelmében. Mivel egy esetleges háborúban Észak-Olaszország volt a Magyar Néphadsereg fő hadműveleti iránya és bevetési területe, ezért a római magyar nagykövetség, illetve a polgári és katonai hírszerzés rendszeresen küldött jelentéseket az olasz hadsereg állapotáról, a haderőfejlesztésekről és a NATO-ban betöltött szerepéről. Ezekben a jelentésekben gyakran megemlítették, hogy Olaszország a NATO leggyengébb tagja.

Kulcsszavak: hidegháború, enyhülés, NATO, Olaszország, katonapolitika, hadsereg

BIHARI RITA

A KONFLIKTUS-FORMÁCIÓTÓL A BIZTONSÁGI KÖZÖSSÉGIG – A NYUGAT-BALKÁNI REGIONÁLIS BIZTONSÁGI EGYÜTTMŰKÖDÉS FEJLŐDÉSE

Mit jelent a biztonsági közösség-formáció? Vajon, hogyan születnek a biztonsági közösségek? Hogyan lehet kialakítani ezt a közösségi formát a Nyugat-Balkánon? A kérdések, amelyekre a tanulmány választ keres, semmiképp sem egyszerűek. Kiindulási pontunk a biztonsági közösség, mint terminus eleve két olyan kifejezést tartalmaz, amelyek meghatározása, habár önmagában egyértelmű, a nyugat-balkáni régióra adaptált változata már másképpen értelmezhető. A Nyugat-Balkánon tapasztalt erőszakos konfliktusok után külső hatásra megindult a régiós szocializáció, amelyben az Európai Uniónak elsődleges szerepe volt. Regionális megközelítése által az EU, a régiós biztonsági együttműködés fejlődésének elősegítésében is prioritást élvezett a térségben érintett további nemzetközi szervezetekkel szemben. A tanulmány átfogó jelleggel kíván számot adni a nyugat-balkáni regionális biztonsági dinamika változásának evolúciós folyamatáról.

Kulcsszó: Nyugat-Balkán, Európai Unió, biztonsági közösség, regionális dinamika

FERENC NEUSPILLER

NATO'S "WEAKEST LINK"? THE MILITARY SITUATION IN ITALY, 1963-1975.

After World War II, Italy committed itself on the side of the Western bloc. Although the Cold War was marked by easing in the 1960s and 1970s, there were still conflicts between the two opposing military alliances and the two superpowers. As one of the founding members of NATO, Italy has played an important role in protecting the Mediterranean and the southern wing of the Alliance. As Hungary would have had to attack Italy in case of a war, the Hungarian Embassy in Rome, just like the civilian and military intelligence regularly sent reports on the state of the Italian armed forces and their developments and its role in the NATO. It has often been mentioned in these reports that Italy is the weakest link of NATO.

Keywords: Cold War, relief, NATO, Italy, military policy, army

RITA BIHARI

FROM CONFLICT FORMATION TO SECURITY COMMUNITY - THE EVOLUTION OF REGIONAL SECURITY COOPERATION IN THE WESTERN BALKANS

What is the safety community formation? How are safety communities created? How can this form of community be developed in the Western Balkans? The questions this study seeks to answer are by no means simple. Our starting point is the term security community, which as a definition contains two terms whose definition, although clear in itself, has a different meaning when adapted to the Western Balkan region. After the violent conflicts in the Western Balkans, the region began to socialise under external pressure, with the European Union playing a primary role. Through its regional approach, the EU also took priority over other international organisations involved in the region in promoting the development of regional security cooperation. This study aims to provide a comprehensive account of the evolution of the changing regional security dynamics in the Western Balkans.

Keywords: Western Balkans, European Union, security community, regional dynamics

DR. KASSAI KÁROLY

A HONVÉDELMI CÉLÚ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK SZÜKSÉGES MÉRTÉKŰ VÉDELMÉNEK BIZTOSÍTÁSA – GONDOLATOK EGY ZÖLD KÖNYV SZÁMÁRA

A katonai információs rendszerek területén hatalmas fejlődés tapasztalható, hasonlóan a világban tapasztalt digitalizációhoz.
Ezzel párhuzamosan reális katonai követelmény a rendszerek, szolgáltatások szükséges mértékű kibervédelmének biztosítása.
Az információbiztonság kérdése NATO-, EU- vagy nemzeti szinten nem tekinthető új kérdésnek.
Az információs rendszerek, szolgáltatások összetettsége, a kiberfenyegetettség dinamikus fejlődése, illetve a katonai képességfejlesztés nehézségei számtalan kihívást jelentenek a kiberbiztonság szempontjából.
A tanulmány áttekinti a magyar katonai képességfejlődés eddigi fontosabb lépéseit, segítve a különböző szempontok azonosítását, a további lépések megalapozását.

Kulcsszavak: kiberbiztonság, elektronikus információbiztonság, áttekintés, biztonságtudatosság, képességfejlesztés

DR. ALBERT ÁGOTA – ÜVEGES ANDRÁS JÓZSEF

AZ „IoT" -ESZKÖZÖK BIZTONSÁGA A SZEMÉLYES ADATOK TÜKRÉBEN

Absztrakt

Mindennapjainkat, a napi munkavégzést, az üzleti életet egyre gyorsuló tempóban alakítja át az információs technológia fejlődése. Az IoT-eszközök száma továbbra is gyors ütemben növekszik, ezen eszközök számának növekedésével a kibertámadások során játszott szerepük is jelentős emelkedést mutat. A globális internetre kapcsolódó, adatgyűjtésre és továbbításra, valamint feldolgozásra, illetve egymás közötti kommunikációra alkalmas okoseszközök az élet számtalan területén radikális változást hoznak majd az ipartól kezdve a közlekedésen át a városok működéséig, illetve a honvédelmi ágazatig. Az IoT kockázati tényezőinek vizsgálata időszerűvé vált mind a honvédelmi, mind pedig a polgári szektorban. Tanulmányunkban ezt a vizsgálatot a személyes adatok tükrében végeztük. Ennek oka, hogy ma elmondhatjuk azt, hogy „az adat az új olaj". Mivel az adatokon alapuló társadalom lendületesebb fejlődést mutatott be az elmúlt évtizedben, mint a fekete aranyat kiaknázó vállalatok 100-150 évvel ezelőtt.

***Kulcsszavak*:** személyes adat, kiberbiztonság, dolgok internete

KÁROLY KASSAI DR.

ENSURING THE NECESSARY SECURITY OF MILITARY ELECTRONIC INFORMATION SYSTEMS – THOUGHTS FOR A GREEN PAPER

There has been huge progress in field of military information systems, similar to the digitization in the world.
At the same time, ensuring the necessary level of cyber protection of systems and services is a realistic military requirement.
The issue of information security is not a new issue at NATO, EU or national level.
However, the complexity of information systems and services, the dynamic development of cyber threats, and the difficulties of military capability development pose numerous challenges to cybersecurity.
The article reviews the most important steps of the Hungarian military capability development so far, helping to identify the various aspects and to lay the foundations for further steps.

Keywords: Cyber security, electronic information security, review; security awareness, capability development

ÁGOTA ALBERT DR. – ANDRÁS JÓZSEF ÜVEGES

SECURITY OF „IoT DEVICES IN THE LIGHT OF PERONAL DATA

The development of information technology is transforming our daily lives, our daily work and our business life at an ever-accelerating pace. The number of IoT devices continues to grow rapidly, and their role in cyber-attacks has also increased significantly as the number of these devices has increased. Smart devices connected to the global Internet, capable of collecting and transmitting data and processing and communicating with each other, will bring about a radical change in many areas of life, from industry to transport to the operation of cities and the defense sector. Examining the risk factors for IoT has become timely in both the defense and civilian sectors. In our article, we conducted this study in light of personal information. The reason for this is that today we can say that "the data is the new oil". Because the data-driven society has shown a vibrant development over the past decade, as companies exploiting black gold 100-150 years ago.

***Keywords*:** Personal Data, cybersecurity, internet of things

SZAKOS JUDIT

VÉDELMI INNOVÁCIÓS ÖKOSZISZTÉMA-FEJLESZTÉS MAGYARORSZÁGON

A tanulmány a magyar védelmi innovációs ökoszisztémát elemzi, amelynek fontossága mind az újonnan megjelenő kettős felhasználású technológiák, mind napjaink globális folyamatainak tükrében megkérdőjelezhetetlen. Az elemzés a szektor specifikumai tükrében az állami beavatkozást, annak stratégia–közpolitika-formáló szerepét emeli ki az intézményi közgazdaságtani értelemben vett intézmények és szervezetek, valamint a Triple Helix- és az MIT 5 dimenziós modell szerinti megközelítésből, jó nemzetközi gyakorlatokat is bemutatva. Ehhez a releváns szakirodalom feldolgozása mellett a hatályos magyar stratégiák elemzésének eszközét alkalmazva.
A tanulmány célja az állami törekvések és egymást erősítő hatások megtalálása a magyar védelmi innovációs ökoszisztémában, amelyek rendszerszinten is élénkítő hatással bírhatnak.

Kulcsszavak: innovációs ökoszisztéma, védelmi innovációs ökoszisztéma, védelmi ipar, állam

ECK GÁBOR – DR. DOBÁK IMRE

A NEMZETBIZTONSÁG INFORMÁCIÓS KÖRNYEZETE

Jelen tanulmány a digitális térben megjelenő adatok és a nemzetbiztonsági ágazat viszonyát vizsgálja, kitekintve a hagyományosan megjelenő információgyűjtő területeket érintő lehetséges változásokra, a kibertérben keletkező információk egyre fontosabb szerepére. Érinti a nemzetbiztonsági tevékenységhez szorosan kapcsolódó egyes információgyűjtési ágak (pld. OSINT, SOCMINT) kérdéseit, a tömeges adathalmazok lehetséges biztonsági célú alkalmazhatóságának lehetőségeit. Nem vizsgálja a titkos információgyűjtés kérdéskörét. Mindezekre a napjaink orosz–ukrán háborúja is számos példával szolgál, jelezve az információs környezet és a hadviselés megváltozott kapcsolatát.

***Kulcsszavak*:** nemzetbiztonság, információ, OSINT, SOCMINT, Crowdsourcing Intelligence, információgyűjtés

JUDIT SZAKOS

DEFENCE INNOVATION ECOSYSTEM DEVELOPMENT IN HUNGARY

This study aims to analyse the Hungarian defence innovation ecosystem. Its importance is unquestionable, both in light of the emerging dual-use technologies and today's global trends. He analysis highlights the state's role in strategic and public policy by considering the sector's specifities and presents some good practices worldwide. With the relevant literature and Hungarian strategies, the framework uses institutional economics, the Triple Helix Model and MIT 5-dimensional Model.
The study aims to identify public efforts and mutually reinforcing roles in the Hungarian defence innovation ecosystemthat could have a systemic boosting effect.

Keywords: innovation ecosystem, defence innovation ecosystem, defence industry, state

GÁBOR ECK – IMRE DOBÁK DR.

OSINT, SOCMINT, CROWDSOURCING INTELLIGENCE

The study examines the relationship between the digital data, information and the national security sector, looking at the changes affecting the traditional areas of information collection and the increasingly role of information generated in cyberspace. It addresses the issues of certain information collection branches related to the intelligence activities (eg. OSINT, SOCMINT), the visible directions of the possible applicability of mass data for security purposes, but does not examine the issue of secret information collection. The recent Russian-Ukrainian war provides many examples of all this, emphasizing the changed relationship between the information environment and warfare.

***Keywords*:** National security, information, OSINT, SOCMINT, Crowdsourcing Intelligence, information collection

SZERZŐINK

Dr. Albert Ágota	adatvédelmi szakjogász
Bihari Rita	Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktorandusz
Babos Sándor	őrnagy, a KNBSZ munkatársa, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktorandusz
Dr. habil. Dobák Imre	nb. ezredes, PhD, Nemzeti Közszolgálati Egyetem, Polgári Nemzetbiztonsági Tanszék vezetője, intézetvezető, egyetemi docens
Eck Gábor	Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktorandusz
Dr. Kassai Károly	ezredes, a KNBSZ munkatársa NKE Katonai Nemzetbiztonsági Kibertér Műveleti Szakcsoport, szakcsoport vezető
Neuspiller Ferenc	Eötvös Loránd Tudományegyetem, Történelemtudományi Doktori Iskola, doktorandusz
Dr. Ritecz György	Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, oktató/Rendészettudományi Doktori Iskola, témavezető
Suhajda Attila	Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola, doktorandusz
Szakos Judit	NKE Eötvös József Kutatóközpont, Amerika Tanulmányok Kutatóintézet, tudományos segédmunkatárs
Tóth Tamás	Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktorandusz
Üveges András József	százados, a KNBSZ munkatársa Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz
Dr. Vida Csaba	ezredes, a KNBSZ munkatársa Nemzeti Közszolgálati Egyetem, Katonai Nemzetbiztonsági Tanszék, egyetemi docens

E SZÁMUNKAT LEKTORÁLTÁK

Dr. habil. Dobák Imre	nb. ezredes, PhD, Nemzeti Közszolgálati Egyetem, Polgári Nemzetbiztonsági Tanszék vezetője, intézetvezető, egyetemi docens
Dr. Forgács Balázs	őrnagy, PhD, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Hadászati Tanszék, tanszékvezető, egyetemi docens
Dr. Fürjes János	alezredes, PhD, a KNBSZ munkatársa
Görbe Attiláné Dr. Zán Krisztina	ezredes, PhD, a KNBSZ munkatársa Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, oktató
Dr. Hódos László	őrnagy, a KNBSZ munkatársa
Dr. Kenedli Tamás	ezredes, PhD, a KNBSZ munkatársa Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, oktató
Keszthelyi Dávid László	alezredes, a KNBSZ munkatársa
Dr. Magyar Sándor	ezredes, PhD, a KNBSZ munkatársa Nemzeti Közszolgálati Egyetem Katonai Nemzetbiztonsági Tanszék, egyetemi adjunktus
Dr. habil. Remek Éva	PhD, Nemzeti Közszolgálati Egyetem, Nemzetközi Biztonsági Tanulmányok Tanszék, egyetemi docens
Dr. Pál István	PhD, Eötvös Lóránd Tudományegyetem, Bölcsészettudományi Kar, oktató
Dr. Vida Csaba	ezredes, PhD, a KNBSZ munkatársa Nemzeti Közszolgálati Egyetem, Katonai Nemzetbiztonsági Tanszék, egyetemi docens

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 (pld. 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.