KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT

XVI. évfolyam 3. szám 2018. október

SZAKMAI SZEMLE

ALAPÍTVA: 2003

BUDAPEST

A Katonai Nemzetbiztonsági Szolgálat
tudományos-szakmai folyóirata

Felelős kiadó

Dr. Béres János altábornagy, főigazgató

Elérhetőségeink

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

HU ISSN 1785-1181

TARTALOM

DR. HABIL. RESPERGER ISTVÁN

AZ ISZLÁM ÁLLAM TERRORSZERVEZET LAKOTT TERÜLETEKEN FOLYTATOTT HARCAINAK KATONAI TAPASZTALATAI[1]

Mottó:
„…harcolni fogunk a tengereken és az óceánokon, harcolni fogunk egyre növekvő bizalommal és erővel a levegőben, megvédjük Szigetünket, bármibe kerüljön, harcolni fogunk a tengerparton, harcolni fogunk a leszállópályákon, harcolni fogunk a mezőkön és az utcákon, harcolni fogunk a hegyekben; sohasem adjuk meg magunkat…”[2]

Winston Churchill

Bevezetés

A Churchill által megfogalmazott mottó minden elemét nem valósította meg az apokaliptikus terrorszervezet, az Iszlám Állam (IÁ), de mindenképpen érdemes az általa megszállt területeken folytatott harci cselekmények, módszerek, eljárások tanulmányozása. Minden katona, rendőr, nemzetbiztonsági szakember számára hasznos tanulságokkal szolgálhat a harci cselekmények elemzése, feldolgozása. Nemcsak a sikeres támadások, offenzívák, de az ellenség által jó módszerekkel végrehajtott támadó és védő tevékenységek is érdeklődésre tarthatnak számot. Kissinger szavai szerint: *„gerilla akkor is nyer, ha nem veszít.”*[3] A hagyományos hadsereg veszít, ha nem győz. Kissinger megfigyelte, hogy a különböző méretű és erőforrásokkal rendelkező hadseregek különböző módon küzdenek. Ez igaz volt az emberi történelem során, de a 20. század közepétől már megjelent az aszimmetrikus hadviselés. Az aszimmetrikus hadviselés akkor áll fenn, amikor a két fő hadsereg egyenlőtlen méretű vagy erejű, továbbá a konfliktus résztvevői nem mindegyike állami fél.

Az Iszlám Állam aszimmetrikus hadviselése elleni küzdelem lehetséges stratégiája

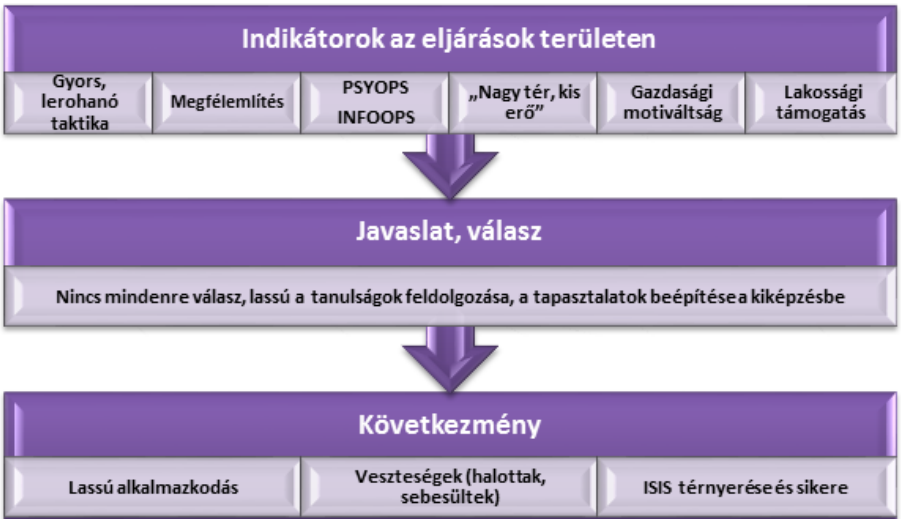
A felmerülő hadtudományi problémákra szeretném a figyelmet ráirányítani. Mivel a hadtudomány elsősorban a fegyverzet, a szervezet és az eljárási módok

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Szélsőségek, vallási szélsőségek Ludovika Kutatócsoport keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

[2] https://moly.hu/konyvek/winston-s-churchill-sohase-engedjetek (Letöltés ideje: 2018. 04. 10.)

[3] https://study.com/academy/lesson/asymmetric-warfare-definition-tactics-examples.html (Letöltés ideje: 2018. 04. 14.)

kérdéseinek megválaszolásával foglalkozik, ezért ezekre a területekre helyezném a fókuszt. Vizsgálati módszerként az ***indikátorokat*** – mint a probléma, a kérdéskör olyan jelzéseit, melyek fontos és meghatározó módon jelzik a hadtudomány területén fellelhető eltéréseket, abnormalitásokat – a lehetséges ***hadtudományi válaszokat, javaslatokat*** és a ***következmények*** bemutatását választom. A módszert a helyiségekben, beépített területeken folytatott harccselekmények elemzésénél alkalmazom.



1. ábra: Indikátorok az eljárások területén
(saját szerkesztés)

2. ábra: Moszul[4]

[4] Forrás: https://www.theguardian.com/cities/2018/mar/26/mosul-struggles-recover-ruins-iraq-isis#img-1, (Letöltés ideje: 2018. 04. 03.)

Az Iszlám Állam kialakulása

A szervezet az al-Kaida nemzetközi terrorszervezetből vált ki, az Abu Muszab al-Zarqawi vezette Jama'at al-Tawhid wal-Jihad[5] nevű szervezethez tartozott, majd vált a térség és sok „esernyőszervezet" vezetőjévé. Mint korábban az al-Kaida, most az IÁ vált a „Pares inter Pares" – „Első az egyenlők között" terrorista szervezetté, amelynek minden nagyobb terrorcsoport hűségesküt tett.[6]

A szervezet egyrészt nagyon gyorsan érte el magas létszámát a harcoló katonáit tekintve, másrészt a területi nyereségei is jelentősek, Rommel észak-afrikai sikereihez hasonlóak. Területileg közel 22-25.000 km^2-t tartott uralma alatt, és ami nagyon fontos, a lakosság támogatását is élvezi, hiszen csak Irak lakosságának 9 millió fője tartozik a szunnita irányzathoz, akik nagyon háttérbe szorultak a 2003-as iraki megszállás után.

A szervezet létszáma alakulása:
2005: 1000 fő,
2006: 1100 fő,
2011: 1000-2000 fő,
2014: 6000-10.000 fő,
2014: 11.000 fő (6000 fő Irakban, 3000-5000 fő Szíriában),
2015: 20.000-31.500 fő.[7]

Az Iszlám Állam vezetése

---

5 HASIM Ahmed, S.: From Al Kaida affiliate to the rise of the Islamic Caliphate: The evolution of the Islamic State of Iraq and Syria (ISIS) RSiS Nanyang Technologial University, 2015. p. 2.

6 A nigériai Boko Haram és a szomáliai al Shabaab 2015 márciusában, a líbiai Iszlám Fiatalok Shura Tanácsa (Islamic Youth Shura Council) még 2014-ben, az afganisztáni tálibok 2015-ben.

7 "Country Reports on Terrorism," United States Department of State, Office of the Coordinator for Counterterrorism, April 2006, retrieved on February 4, 2010 from http://www.state.gov/documents/organization/65462.pdf, p. 220. (Letöltés ideje: 2015. 09. 20.)
TILGHMAN, Andrew, "The myth of AQI," Washington Monthly, October 2007, retrieved January 26, 2010 from http://www.washingtonmonthly.com/features/2007/0710.tilghman.html (Letöltés ideje: 2015. 09. 20.)
Country Reports on Terrorism 2011." U.S. Department of State. Published July 31, 2012. http://www.state.gov/j/ct/rls/crt/2011/195553.htm#ig, (Letöltés ideje: 2015. 09. 20.)
Accessed August 2, 2012., {Zahiyeh, Ehab. "How ISIL became a major force ith only a few thousand fighters." June 19, 2014, retrieved June 23, 2014 from http://america.aljazeera.com/articles/2014/6/19/isil-thousands-fighters.html, (Letöltés ideje: 2015. 09. 20.)
The Economist: The Islamic State of Iraq and Greater Syria: Two Arab counties fall apart, The Economist. June 13, 2014, retrieved June 23, 2014 from http://www.economist.com/news/middle-east-and-africa/21604230-extreme-islamist-group-seeks-create-cal, (Letöltés ideje: 2015. 09. 20.)
YEGINSU, Ceylan: ISIS Draws a Steady Stream of Recruits From Turkey. The New York Times. 15 Sept. 2014. Web. 11 Nov. 2014., http://www.nytimes.com/2014/09/16/world/europe/turkey-is-a-steady-source-of-isis-recruits.html,(Letöltés ideje: 2015. 09. 20.)

A szervezet vezetője Abu Bakr al-Baghdadi, aki egy Súra Tanácsot (13 tagú), egy katonai tanácsot (13 tagú), egy hírszerző és felderítő tanácsot vezet. Emellett a másik pillért a vallási tanács és az alárendelt vallási rendőrség képezi. Ők, akik a leghatározottabban megőrzik az iszlám alapjait, az ellene vétkezőket a helyszínen kivégzik. Baghdadi önmagát az állam kalifájának nevezi. Kettő helyettese – akik helytartók Irakban és Szíriában –, továbbá a megszállt területeken 13 szíriai és iraki tartományt irányító kormányzó, közel 1000 középvezető irányítja az IÁ lakosságát. Ők 300-2000 USA dollár havi ellátást kapnak a vezetéstől, melyek járulékokkal egészülnek ki a harcos feleségének és gyermekeinek számától függően.[8]

Katonai tanácsa, a különböző (katonai, gazdasági, adminisztrációs, terror, pénzügyi és információs) műveletekért felelős, ennek gerincét azok a tisztek alkotják, akik a Szaddam Husszein-rendszer szunnita kisebbségi tagjai, a korábbi rendszer katonai, rendőri, politikai, titkosszolgálati vezetői voltak.[9] A kabinet tagjai a hadi ügyekért, fegyverzetért, külföldi harcosokért, öngyilkos merénylőkért, általános biztonságért, foglyokért, koordinációért, adminisztrációért, pénzügyekért, szociális szolgáltatásokért felelősek. Szóvivőjük a szíriai Abu Mohammed al-Adnani[10] Az Iszlám Állam igazi erejét a külföldi harcosok alkotják. A dzsihadisták közel 80 országból érkeztek, létszámuk közel 20.000 fő. Külföldi harcosok a következő országokból érkeztek: Szaúd-Arábia 2500, Tunézia 3000, Marokkó 1500, Franciaország 1200, Németország 600, Jordánia 1500, Oroszország 1500 fő, Törökország 1000 fő.[11] A fegyveresek közül sokan rendelkeznek harci tapasztalatokkal, amelyeket az al-Kaida kötelékében, vagy a szíriai, esetleg az iraki hadseregben szereztek, ahonnan dezertáltak. Az Iszlám Állam létszáma elsősorban más dzsihadista csoportok beolvasztása, illetve a törzsek tagjainak befogadása révén nőtt meg. Mit kínál az IÁ? Elsősorban az erőszak, a brutalitás kiélésének lehetőségét. Sikert és lehetőséget kínál arra, hogy a sok vereséget, megaláztatást elszenvedett muszlim harcosok győztes szerepben jelenjenek meg, alakítsák a térség sorsát. Az újoncok először alapos kiképzésen vesznek részt, majd ezután kerülnek be a hatékony katonai szervezetbe. Műveleteikben a mobilitás, a felőrlés és a terror elegyét alkalmazzák. Különösen hatékonynak bizonyult, amikor kisebb, mozgékony katonai alegységekkel meglepetésszerű támadásokat indítottak egy területen. Emellett nem mondanak le a féktelen apokaliptikus terrorról sem. De facto fővárosukként a szíriai Rakkát jelölik meg.

---

8 Special Report: Islamic State p. 18.

9 Vezetőik: Abu Bakra al-Baghdadi, Ibrahim Awwad Ibrahim Ali al-Badri al-Samarai, az IÁ vezetője; Fadil Ahmad Abdallah Hayyali aka Abu Muslim al-Turkmani, Baghdadi helyettese, alezredes egykor a Száddam korszakban; Abu Ayman al-Iraqi aka Abu Mohammad al-Sweidawi, a katonai tanács egyik tagja, egykori ezredes a légierő hírszerzésénél; Abu Qasim aka Abdullah Ahmad al-Masshadani, a külföldi harcosok és az öngyilkos merénylők toborzója; Abu Lu'ay aka Abdul Wahid Khutnayer Ahmad, biztonsági főtiszt; Abu Shema aka Fares Raif al-Naima, áruházak és ellátás felelőse; Abu Suja aka Abdul Rahman al-Afari, a szponzorálások és a mártírok családjainak felelőse. Forrás: BARRETT Richard: The Islamic State p. 24. http://soufangroup.com/wp-content/uploads/2014/10/TSG-The-Islamic-State-Nov14.pdf (Letöltés ideje: 2015. 09. 27.)

10 HERRMAN, Rainer: Az Iszlám Állam, A világi állam kudarca az arab világban, pp. 30-32. BARRETT i. m. pp. 29-32.

11 http://mno.hu/kulfold/nem-ker-az-iszlambol-a-britek-tobbsege-1280069 (Letöltés ideje: 2015. 09. 26.), BARRETT i. m. p. 16.

Az Iszlám Állam stratégiája

A szervezet ellenségei egyes csoportjai ellen klasszikus terrorakciókat követ el, a lehető legtöbb ember megölésével a lehetséges legnagyobb félelmet kelti. A célzott gyilkosságok és kivégzések az ellenség elrettentését szolgálják, amihez az is hozzátartozik, hogy az első alegység a meghódított városban azonnal önkényes kivégzéseket hajt végre a főtéren, amely a félelemkeltés mellett azt a célt is szolgálja, hogy elmeneküljön a lakosság egy része. Mivel az Iszlám Állam propagandarészlege videókat terjeszt az efféle mészárlásokról, a meghódított területek lakossága tudja, hogy mire számíthat.[12] A szervezet másik arca a lakosságot segítő, annak egészségéért és jólétéért cselekvő tevékenysége. Például a gyermekbénulás elleni oltóanyag mellett indítottak kampányt. Lényegében a régi amerikai „Shock and Awe" – Sokkoló és lefejező csapások – stratégiát valósítják meg.

Az újoncokat táborokban képzik ki. Ilyen táborok nyilvánvalóan minden nagyobb városban működnek, amely az Iszlám Állam ellenőrzése alatt áll. A dzsihádisták abban a biztos meggyőződésben indulnak egy-egy ütközetbe, hogy ha elesnek, „vértanúk" (sáhidok) lesznek, így bizonyosan a Paradicsomba jutnak, és haláluk révén halhatatlanná válnak. Az, hogy a „hitetlenek" megölése során készek maguk is meghalni, mindenféle párbeszédet lehetetlenné tesz velük. Az empátiára és a gyászra való képesség kiveszett belőlük; gyönyörűségüket lelik a gátlástalan erőszakban, még gyerekek és nők lefejezésében is.

Az Iszlám Állam fennmaradásának második oka hatékony katonai szervezetében keresendő. Abu Bakr al-Bagdadi már a börtönben toborozni kezdte az amerikai megszállás idején lecsukott volt iraki tiszteket azzal, hogy ők értenek a klasszikus hadvezetéshez, a megtévesztéshez, a felforgatáshoz. (A 2003-ban felszámolt iraki hadsereg volt tisztjeit csak azzal a feltétellel vették fel a szervezetbe, ha kijelentették, hogy „megbánták" tettüket és hűségesküt tettek.) Az al-Kaida volt harcosai ugyanakkor a gerillaharcban rendelkeznek jártassággal.[13]

Tevékenységük tervezésénél a volt szovjet/orosz iskola hadműveleti, harcászati elveit, felforgató és mélységi műveleteket, az afgán, iraki és egyéb hadszínterek tapasztalatait fedezhetjük fel. Az aszimmetrikus hadviselés minden elemének – reguláris erők (lövész, harckocsizó, tüzérség) a könnyű fegyverzetű alakulatok, irreguláris csapatok, az információs hadviselés – alkalmazása mellett a közösségi média[14] minden spektrumát kihasználják. Az IÁ stratégiájának egyik fontos eleme, hogy működési területén mindig az ellenőrzött zóna, támogató zóna és a támadott zóna felosztást alkalmazza. A szervezet súlypontját (Center of Gravity – CoG) a szervezet külföldi harcosai, dzsihádistái és a szunnita lakosság képezi. A tervezésnél a rommeli gyors, mozgékony csapások, a magas helyiértékű pontok (olajmezők, gázmezők, gátak, nagyobb városok, kritikus erőforrások)[15] irányába történő

---

12 RAINER i. m. p. 56.

13 U.o. pp. 58-60.

14 WINTER, Charlie: The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf, pp. 18-21. (Letöltés ideje: 2015. 11. 25.)

15 BARRETT i. m. p. 52.

előrenyomulás a meghatározóak. Ezt követően a „Tisztítsd meg, építsd ki, tartsd meg” (clear-build-hold) elvek mentén haladnak tovább. Erősségei a könnyű fegyverzet, a jó felderítés és kommunikációs képességek,[16] mozgékonyság, tűzerő, robbanóeszközök alkalmazása és a lakossági támogatás. A tervezésnél alapelv a teljes körű média-jelenlét a lakossági támogatás megszerzése érdekében.

A saját (NATO erők, szövetséges csapatok) és az ellenség (ISIS és szövetségesei) képességei értékelésénél a műveleti ütemüket, lakossági támogatásukat, robbantásos cselekményeiket és információs műveleteiket kell kiemelnünk.

3. ábra
(saját szerkesztés)

IÁ stratégiája az, hogy úgy törekszik a katonai végállapotra, hogy nem a katonai győzelem elérése a cél, hanem a nyugati erők kivonulása. A szervezet megtörni, kifárasztani és kivéreztetni akarja a saját erőinket az aszimmetrikus és gerilla-hadviselés, illetve a terrorizmus módszereivel a teljes információs hadviselés alkalmazása mellett, amellyel a közvéleményünkre „mér csapást”.

[16] A Twitteren 2014-ben 50.000 követőjük volt, a napi tweet-ek száma 2013. 09. 17-10. 17. között 100.000- 250.000 darabot tett ki. Forrás: BARRETT i. m. p. 59.

Az Iszlám Állam lakott területeken és a beépített területeken folytatott hadviselésének katonai tapasztalatai

Moszul eleste és a moszuli gátrendszer védelme hadtudományi szempontból

4. ábra: Az ISIS támadói Moszul ellen[17]

Az IÁ Moszul elleni támadását nagyon kevés létszámú terrorista (100-200 fő) hajtotta végre, több irányból benyomulva a városba. Az iraki biztonsági erők (közel 3000 fő!), azonnal visszavonult és a várost feladta. Sajnos 3000 harc- és gépjárművet hagytak hátra, továbbá rengeteg katonai felszerelést. Ezen túl a moszuli bank 450 millió dolláros készlete is a kezükre jutott. Katonai szempontból az iraki biztonsági erők leszerepeltek, Észak-Irak második legnagyobb városa elesett a környezetében levő stratégiai víztartalékokkal a moszuli gátrendszerrel együtt.

IÁ által használt fegyverek és fegyverrendszerek:[18]

- Harckocsik: T-55, T-62, T-72,
- Páncélozott szállító harcjárművek: BMP-1, BTR-60, BTR-80,
- Páncélozott járművek: tehergépkocsik átalakításával,
- Tüzérségi eszközök: M 198 önjáró löveg, 59-1 tábori tarack,
- Rakéták: SCUD hadműveleti rakéta,
- Páncéltörő eszközök: RPG-7, RPG-29 kézi páncéltörő fegyver, M79, KOMET, HJ-8, páncéltörő rakéták,
- Légvédelmi eszközök: DSK légvédelmi géppuska, ZU 23-2 légvédelmi gépágyú, FIM 92 STINGER, SA-16, SA-7, FN- 6 MANPADS kézi légvédelmi rakéták.

---

[17] Forrás: https://www.rt.com/news/263769-iraq-isis-humvees-weapons/ (Letöltés ideje: 2018. 04. 15.)

[18] WILSON, Jeremy – ROSEN, Armin – BENDER Jeremy: These are the weapons Islamic State fighters are using to terrify the Middle East, In: https: uk.businessinsider.com/isis-military-equipment-arsenal-2016/#social-media-27 (Letöltés ideje: 2018. 04. 27.)

Moszul visszavételének katonai tapasztalatai (2016. október-2017. július)

A stratégiai elhelyezkedésű város visszavétele céljából a megreformált iraki biztonsági erők dandár, zászlóalj harccsoportokat hoztak létre katonai és rendőri erőkkel. A harccsoportok fegyverzete a könnyű katonai járművekből (HUMVEE), a nehéz harckocsikból (M1 ABRAMS), a támogató tüzérségi eszközökből, (122 m-es, 155 mm-es tarack, 122 mm-es önjáró tarack) állt.

A műveleteket egységes műveleti parancsnokság tervezésével, vezetésével és külföldi (amerikai, brit) tanácsadók bevonásával hajtották végre. Az IÁ elleni koalíció létrehozása óta közel 20.000 iraki katonát készítettek fel az USA tanácsadói a terrorszervezet elleni küzdelemre.[19] Szorosan együttműködtek a kurd pesmerga katonai erőkkel a műveletek végrehajtása során.

Ekkor az iraki biztonsági erők felépítése a következő volt:[20]

Iraki Szárazföldi Hadsereg (Iraqi Army-IA)

- 1 harckocsi hadosztály
- 4 gépesített hadosztály
- 3 gépkocsizó hadosztály
- 1 lövész hadosztály
- 2 lövész dandár
- 1 parancsnoki hadosztály
- 100.000 fő

Légvédelmi Parancsnokság (Air Defense Command- ADC)

- 2 légvédelmi hadműveleti központ alakult meg a tervezet 4-ből
- 4000 fő

Iraki Légierő (Iraqi Air Force-IqAF)

- 8 repülőszázad alakult meg a tervezett 24-25-ből
- 5000 fő

Iraki Haditengerészet és Tengerészgyalogos Erők (Iraqi Navy and Marines-IqN/M)

- 1-1- haditengerészeti dandár és tengerészgyalogos dandár
- 3600 fő

Terrorizmusellenes Szolgálat (Counter Terrorism Service-CTS)

- 8-9 zászlóalj jött létre a tervezett 21-ből
- 2 dandár alakult meg a tervezett 7-ből
- 5000 fő

---

[19] https://www.washingtonpost.com/world/in-baghdad-us-defense-secretary-to-size-up-iraqi-forces-will-to-fight/2015/07/23/384b284e-30ad-11e5-a879-213078d03dd3_story.html (Letöltés ideje: 2015. 12. 12.)

[20] Military Balance 2015. Szerk.: NEAMAN, Rachel, The Institute for Strategic Studies London, 1996. pp. 330-331.

Szövetségi Rendőrség (Federal Police-FP)

- a 14 tervezettből 6 szövetségi rendőr hadosztály alakult meg
- 43.000 fő
- 5 szektorban egy-egy hadosztályszintű gépesített és haditengerészeti határőr erő került létrehozásra
- 60.000 fő

Olaj Rendőrség Igazgatóság (OPD-Oil Police directoriate)

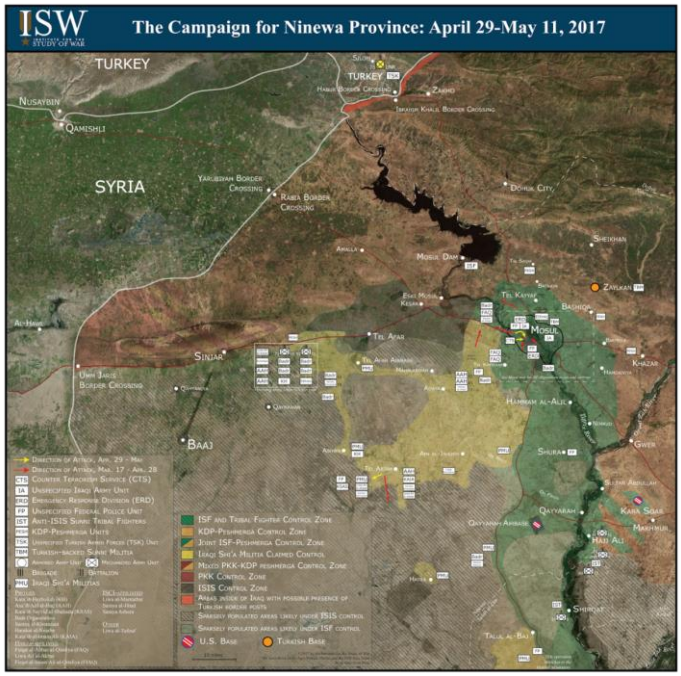
- 4 igazgatóság került kialakításra
- 3 infrastruktúra védelmi szolgálat (95.000 fő)

Kurd Regionális Gárda (Kurd Regional Guards-KRG)

- 8 dandár alakult meg a tervezett 26-ból
- 5000 fő

Az iraki fegyveres erők 270 harckocsival (130 M1A1 Abrams, 120 T 72, 50 T-55), 4000 páncélozott harcjárművel, 1061 tüzérségi eszközzel, 81 többcélú, illetve szállító helikopterrel, továbbá 10 felderítő és 13 harcihelikopterrel rendelkeznek. A légierő 77 eszközzel rendelkezik (többségében kiképző és szállító gépekkel, Cessna, C-130 Hercules stb.), csapásmérő erőt csak a SZU-25 csatarepülő század hét gépe jelent. A legnagyobb biztonsági erő felett a Belügyminisztérium rendelkezik (531.000 fő), a rendőrség állománya ebből 302.000 fő.[21]

Műveletek Ninive tartományban:



5. ábra: Harcok Ninive tartományban[22]

[21] Military Balance 2015. pp. 330-331.

[22] Forrás: http://iswresearch.blogspot.hu/search/label/Iraq (Letöltés ideje: 2018. 04. 10.)

A hadműveleti terület jellemzője volt a többnemzetiségű alkalmazás. A török, a kanadai különleges erők, a kurd pesmergák és az iraki reguláris katonai és rendőri erők alkalmazása. Ezek mellett a síita milíciák, a török-síita vegyes kötelék vett részt a tartomány megtisztításában. A szárazföldi offenzívát az USA által támogatott USA-iraki CJTF kötelék vezette. A brit királyi Légierő (Royal Air Force) a szárazföldi művelet megkezdése előtt 72 órával, már Royal Air Force's drónokkal, kazettás lövedékekkel, tüzérséggel pusztította az IÁ állásait. Az iraki vezetésű koalíciót 94.000 főre becsülték, ami később 108.500 főre nőtt. Az iraki erők 54.000-60.000 főt, a kurd erők közel 40.000 peshmerga harcost tettek ki. Az iraki és a peshmerga erők a moszuli művelet időszakában 10:1 arányú erőfölénnyel rendelkeztek az IÁ ellen. Az iraki hadsereg propagandával szerette volna elérni, hogy a város lakói kezdjenek harcokat az IÁ ellen. A támadásokkal szembeni védelmi felkészítés érdekében az IÁ szakemberei 4 millió lyukat készítettek elő a város körül, melyeket olajjal akartak feltölteni és meggyújtani a láthatóság csökkentése érdekében. Emellett a Moszul-környéki falvakban több robbanásveszélyes alagutat készítettek elő menekülőshez és robbanószerkezeteket berobbantáshoz, csapdákat és rögtönzött robbanóeszközöket (IED). Jelentős aggodalomra ad okot, hogy az IÁ vegyi fegyvereket alkalmazhatnak katonák és civilek ellen.

Adatok a légicsapásokról

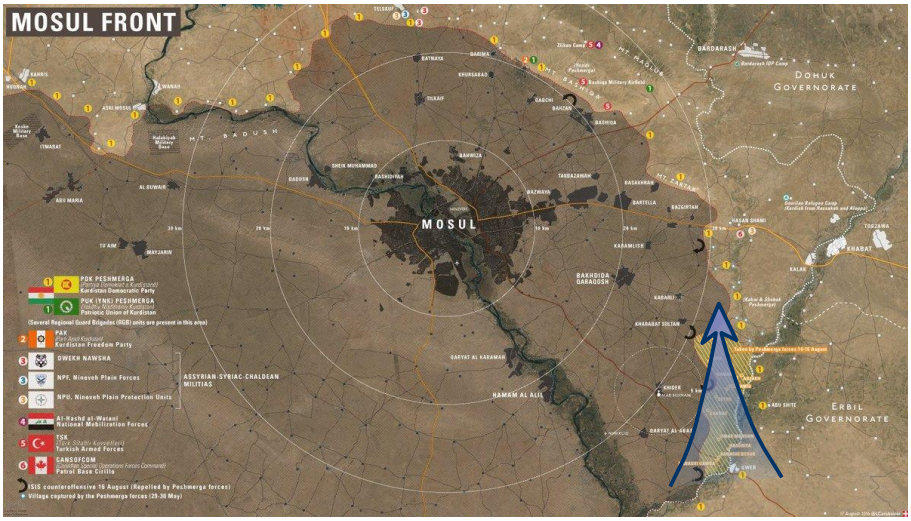
Légicsapások az IÁ mesterlövészeire: 51 db, a támadás légicsapásokkal történő támogatása: 18 db.

A sárgával jelölt területeken (lásd 6. ábra) síita milíciák, a zöld az iraki fegyveres erők által, a pirossal jelzett területek pedig kurd ellenőrzés alatt álltak.

Moszul köré az iraki fegyveres erők, a síita milíciák és a kurd erők vonultak fel, a várost kettő oldalról bekerítve. a sávhatár az előretörő csapatok között a TIGRIS folyó volt.

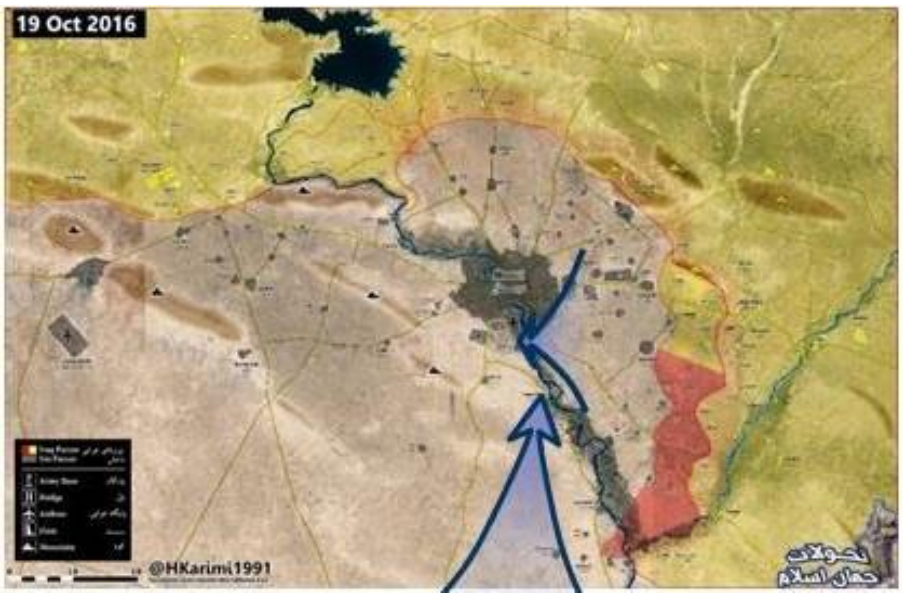
A moszuli front

A város irányába mért első csapás, a bekerítő művelet első részét képezte. A támadást a TIGRIS folyótól keletre tevékenykedő kötelék végezte. Támadási irányuk az OVER-KASARI volt. A művelet célja az volt, hogy a kurd erőkkel felvegyék az összeköttetést és előrenyomuljanak a város keleti oldalához. Az Egyesült Államok Védelmi Minisztériuma szerint mintegy 3000-5000 IÁ harcost találtak Moszul városban. Más becslések 2000-12 000 IÁ harcost adott meg. A Mosul Eye becslése szerint körülbelül 8 000-9 000 harcos volt, akik hűek voltak az IÁ-hoz.



6. ábra: A moszuli front[23]

A területen a kurd erők egy kelet-nyugat irányú offenzívát indítottak azzal a céllal, hogy az iraki kormányerőkkel megteremtsék az összeköttetést, és a további műveletekhez kedvező feltételeket teremtsenek a város keleti oldalán.



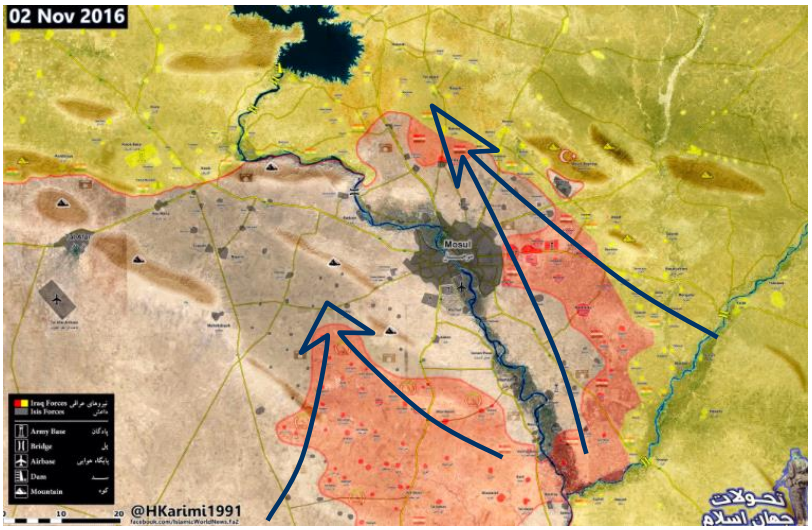
7. ábra: az iraki és kurd erők előrenyomulása Moszulhoz – 2016. 10. 19.[24]
(Megjegyzés: fekete szín: IÁ állása, piros szín: iraki erők, sárga szín: kurd pesmerga erők)

---

[23] Forrás: https://southfront.org/iraqi-map-update-battle-for-mosul-on-november-8-2016/ (Letöltés ideje: 2018. 04. 10.) Kiegészítéssel ellátta a szerző.

[24] Forrás: https://www.almasdarnews.com/article/battle-mosul-enters-day-three-isis-consolidates-frontline-map-update/ (Letöltés ideje: 2018. 04. 10.) Kiegészítéssel ellátta a szerző.

A művelet második ütemében a terroristaellenes erők kétoldalú csapással, egyik irányban HAMAM AL ALIM-BADUSH D 8 km (nyugati oldal), másik irányban a BARKHIDA-TILKAIF (keleti oldal) mértek csapásokat és a várostól 5-7 km-re jutottak ki. A terroristák főként a lakott településeken fejtettek ki ellenállást, folyamatosan vonultak vissza erőik Moszul irányába. Apróbb ellenlökéseket hajtottak végre, öngyilkos merényleteket végeztek gépkocsival, könnyű harcjárművel végrehajtva.



8. ábra: Az iraki és kurd erők előrenyomulása Moszul városhoz – 2016. 11. 09.[25]
(Megjegyzés: fekete szín: IÁ állásai, piros szín: iraki erők, sárga szín: kurd pesmerga erők)

A létrehozott katonai alegységek és egységek az ideiglenes IÁ-ellenes koalíció folyamatos légi felderítése és légicsapásai mellett tevékenykedtek. A műveletek lefolyása a következő volt:

- légicsapások végrehajtása, célzott precíziós csapások végrehajtása;
- az iraki biztonsági erők felzárkózása az IÁ vonalaihoz (2-3 km-re);
- további stratégiai és harcászati UAV-ok alkalmazása felderítésre, csapásmérésre;
- a támogató tüzérségi eszközökkel, harckocsikkal egyes célok, körletek megsemmisítése, pusztítása, tűzzel történő manőverezés (tűzösszpontosítások, a támadó csapatok tüzérségi tűzzel történő támogatása, a mélységi harc tüzérségi tűzzel történő támogatása;
- csapatokkal történő manőverezés, az IÁ állások oldalába, szárnyába irányuló manőverek (átkarolás, megkerülés) a közös rendőri katonai harccsoportokkal;

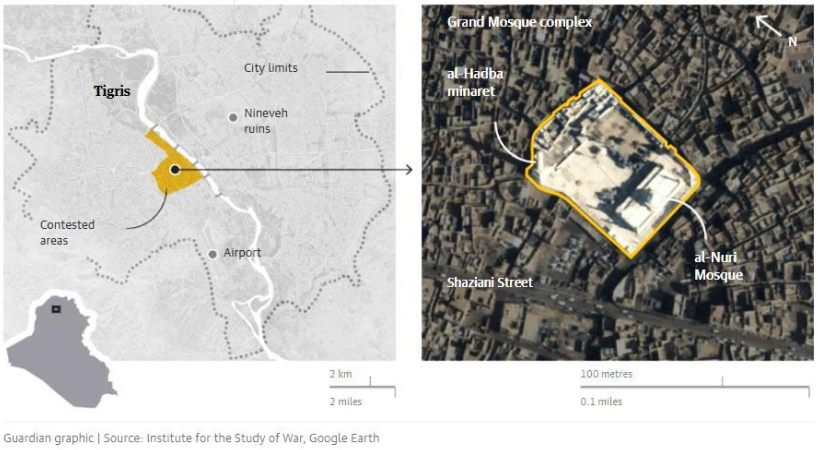
[25] Forrás: https://www.almasdarnews.com/article/battle-mosul-enters-day-three-isis-consolidates-frontline-map-update/ (Letöltés ideje: 2018. 04. 10.) Kiegészítéssel ellátta a szerző.

- műszaki alegységekkel megerősített harccsoportok által a műszaki zárakon átjárók nyitása és megerődített körletek mentesítése az rögtönzött házi készítésű robbanó eszközeitől, a csapatok támadási irányában és a támadási céljai irányában;
- a harccsoportok előrevonása, manőverezés tűzzel, az IÁ harcosainak lefogása, megsemmisítése;
- előremozgás a védett körzet, város, lakott, beépített terület mélységébe, együttműködve a többi harccsoporttal;
- további felderítés és csapásmérések, az ellenség helyzetének, állásainak pontosítása;
- esetenként a harckocsik előrevonása, tűzcsapások végrehajtása, manőver az ellenség mélységébe;
- az elfoglalt területek biztosítása a második lépcső, vagy a tartalék katonáival;
- a terület műszaki alegységekkel történő ellenőrzése;
- a menekülő lakosság biztonságos zónákba történő telepítése, ellátása vízzel, élelemmel, egészségügyi segélynyújtás;
- a támogató tüzérségi erők alkalmazása az IÁ állásai ellen;
- a harccsoportok következő támadási céljainak pontosítása;
- a manőverek végrehajtása a következő IÁ állások birtokbavételére.

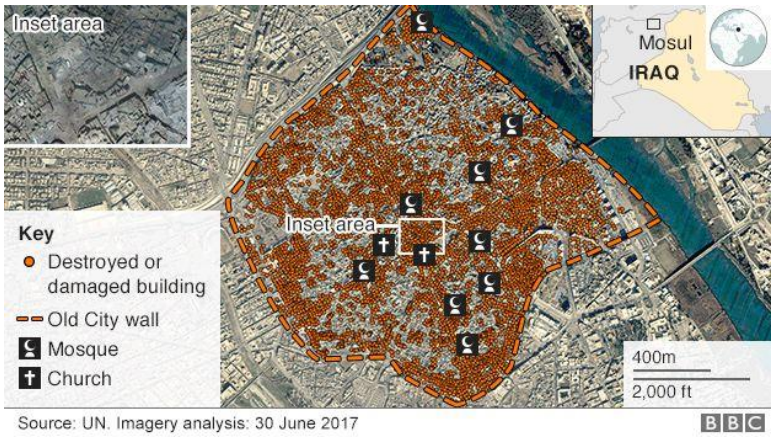
A moszuli műveletek egyik legnehezebb részét a civil lakosság evakuálása, a segítségnyújtás jellemezte. Katonai szempontból az ellenség védelmi súlypontját az Öreg Városrész védelme, a moszuli nagymecset körzetének megtartása képezte. Itt a kis alegységekre (7-10 fő) osztott IÁ-kötelékekkel megvalósuló, a beépített településeken zajló, házról-házra történő küzdelem folyt. A rengeteg vallási emlékhely, mosé (8 darab) és kettő templom a kis területen (2x1 km) nehezítette az IÁ állam harcosainak semlegesítését. A terület egyik oldalát a Tigris-folyó határolta, ez meg is határozta a harcok kimenetelét a terroristák részére, innen nem volt hová visszavonulni. A területen levő épületek közel 80%-át teljesen lerombolták a harcok folyamán. A műholdképek felhasználásával az UNITAR-UNOSAT összesen 2.589 sérült vagy elpusztult épületet azonosított.[26]

[26] FLAMOTHE Dan – GIBBONS-NEFF Thomas – KARKLIS Laris – MEKO Tim: Battle of Mosul: How Iraqi forces defeated the Islamic State, In: https://www.washingtonpost.com/graphics/2017/world/battle-for-mosul/?utm_term=.bd9dab107241 (Letöltés ideje: 2018. 04. 10.)

A moszuli nagymecset komplexum elfoglalása



9. ábra: Az Öreg Város Moszulban és a nagymecset komplexum[27]



10. ábra: Az Öreg Város templomai, moséi, rombolt épületei[28]

[27] Forrás: http://www.bbc.com/news/world-middle-east-37702442 (Letöltés ideje: 2018. 04. 10.)

[28] Forrás: http://www.bbc.com/news/world-middle-east-37702442 (Letöltés ideje: 2018. 04. 10.)

11. ábra: Irak fontosabb víztározói és gátrendszerei[29]

12. ábra: A moszuli gát[30]

A gát eleste sok aggodalomra adott okot, ugyanis ha azt felrobbantják, akkor az így kialakuló 20 méter magas hullámok több lejjebb fekvő várost és falut is veszélyeztethettek volna.

[29] Forrás: Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf, p. 17. (Letöltés ideje: 2018. 04. 14.)

[30] Forrás: https://www.usatoday.com/story/news/world/2017/05/30/iraq-government-has-yet-decide-if-renew-critical-work/102198756/ (Letöltés ideje: 2018. 04. 14.)

13. ábra: A moszuli gát, az IÁ terrorszervezet megszállásakor[31]

Augusztus 16-án az USA légi támadása mellett a kurd csapatok is megtámadták az IÁ-ot, lőtték a közelben lévő állásokat, így megnyitották az utat egy későbbi szárazföldi akció előtt. A támadásokban az ISIL 500 harcosa közül legalább 11 tagját megölték. Az amerikai légierő eddig a napig kilenc légi támadást indított, melyben négy páncélos csapatszállítót, egy páncélozott járművet, hét harckocsit, és két Humvee-t megsemmisített vagy megrongált. Az ISIL katonái robbanó eszközökkel próbálták lelassítani a kurdok előrenyomulását, melyek között voltak házi készítésű bombák és taposóaknák is.

A gátrendszer védelmi terve megmutatja az IÁ katonai, harci tapasztalatait, a különböző válságövezetekben, a csecsen, az afganisztáni, az iraki és a szíriai polgárháborúban szerzett tapasztalatokat. A védelem terve az összes tűzzel, manőverrel végezhető momentumot tartalmazza, a műszaki zárrendszerrel, a tereppel szoros összhangban.

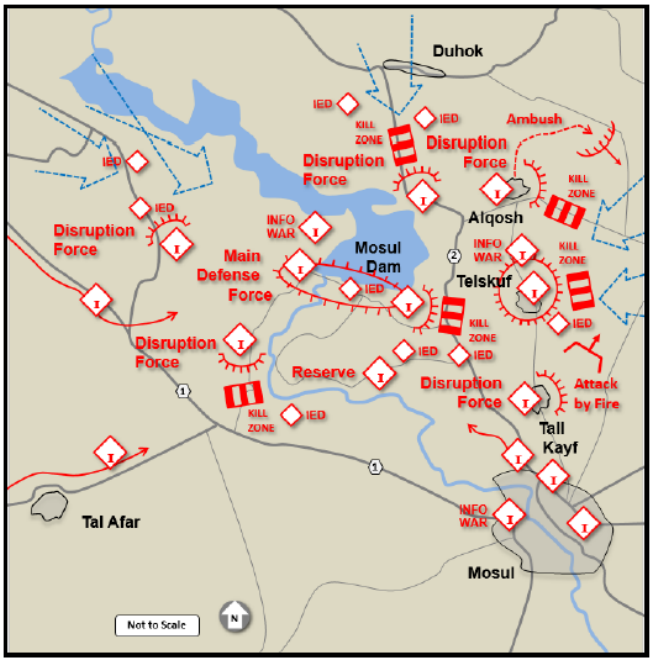
Ezek a következőek voltak:

- biztosító erők állásai,
- előretolt állások,
- harcelőőrsök,
- fő védelmi terepszakasz (peremvonal),
- a második védelmi terepszakasz,
- a megerődített körletek,
- tűzösszpontosítási körletek,

IED-k alkalmazási körletei:

- a szakasz megerődített körletek,
- a tartalékok körletei,
- a második lépcső, tartalékok ellenlökési terepszakaszai, tűzszakaszai,
- a műszaki zárrendszer,
- az ellenség tűzzel történő pusztításának terepszakaszai, körletei (halálzónák),
- az ellenség, szárnyába, hátába tervezett manőverek,
- a műszakilag előkészített manőver utak.

[31] Forrás: https://www.almasdarnews.com/article/isis-positions-hammered-mosul-families-flee/ (Letöltés ideje: 2018. 04. 14.)



14. ábra: A moszuli gátrendszer védelmének felépítése[32]

DARAA városért folytatott harcok

Az első kormány offenzíva 2011. 04. 25 - 05.15.

A hadművelet kezdetén szíriai katonák – harckocsik támogatásával – megszállták a kormányellenes tüntetések központjának számító dél-szíriai Dara várost. A városban összecsapásokra került sor a hadsereg és az ellenzéki tüntetők, illetve ellenzéki fegyveresek között. A harcokban közel 50-220 ellenzéki és 106 katona, esett el.[33] A harcok végül a hadsereg győzelmével értek véget. Az első művelet tapasztalatai:

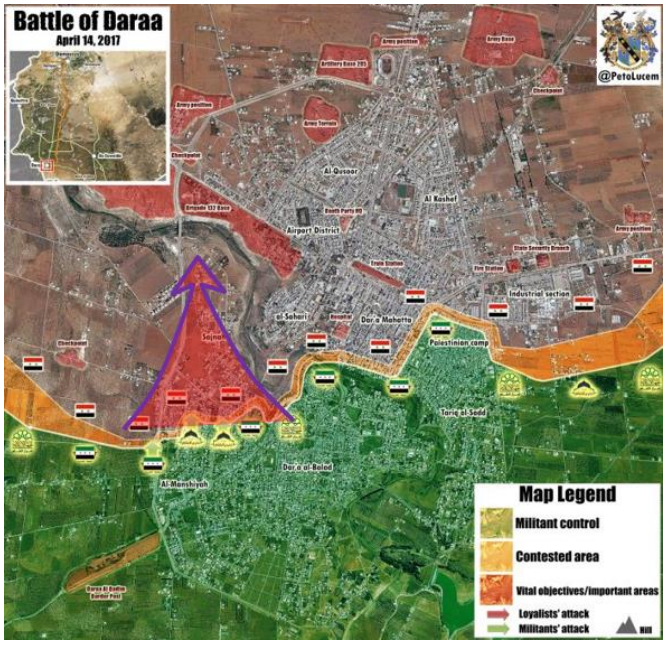
- a kormányerők a katonák támadását, harckocsik alkalmazásával segítették,
- több alkalommal került sor nehézgéppuskák, alkalmanként gépágyúk alkalmazására,
- mesterlövészek alkalmazása,
- a víz, energia korlátozása és a határ lezárása,
- a vallási központ (mecset) elfoglalása törte meg a várost védő felkelőket.[34]

---

[32] Forrás:Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf p. 5. (Letöltés ideje: 2018. 04. 14.)

[33] http://www.nytimes.com/2011/04/26/world/middleeast/26syria.html?_r=1&hp (Letöltés ideje: 2018. 04. 10.)

[34] Analysis: The Battlefield in Syria's Southernmost City, Daraa, In: https://www.newsdeeply.com/syria/articles/2017/06/23/analysis-the-battlefield-in-syrias-southernmost-city-daraa (2018. 04. 10.)



15. ábra: DARA városért folytatott harcok[35]

A felkelők támadása

A városban a jól elkülöníthető frontvonal két oldalán a szíriai kormányerők és a felkelők harcoltak (narancssárga terület a térképen). Az arcvonalban megerődített körleteket találhatunk. A felkelők támadása nem sok sikerrel járt, inkább átmeneti területnyereségek voltak. A kormányerők folyamatos légicsapásokkal, ellenlökésekkel, tűzcsapásokkal pusztították őket.

A felkelők pusztításában az orosz légierő több tucat légi csapást hajtott végre a felkelők pozíciói ellen. Másnap a hadsereg ellentámadást indított, melyben Manshiyah több részét is visszafoglalta.

A hadsereg ellentámadása

Február 20-án a felkelők felújították támadásaikat. Aznap azonban az a Khalid ibn al-Walid Hadsereg kihasználta a felkelők erőinek átcsoportosításából fakadó lehetőséget, támadást indított Daraa területétől nyugatra, a felkelők ellen. Három napnyi támadás során 132 embert öltek meg.[36] Február 25-én a felkelők egyik rakétatámadása megsemmisítette a Muawiyas iskolát Manshiyah kerületében. Aznap a Köztársasági Gárda 500 gyalogosból álló erősítése megérkezett Daraa területére, mely a kormányerők ellentámadását jelezte előre. A támadás több épületet is visszafoglalt Manshiyah területén.[37]

---

35 Forrás: https://www.almasdarnews.com/article/updated-battle-map-of-daraa-city-southern-front-brigades-on-the-offensive/ (Letöltés ideje: 2018. 04. 10.)

36 FADEL, Leith: Syrian Army turns the tables on the jihadist rebels in Daraa, several points recaptured: video, al-Masdar News, (Letöltés ideje: 2018. 04. 10.)

37 TOMSON, Chris: Modest gains as the Syrian Army continues Daraa counter-offensive, al-Masdar News (Letöltés ideje: 2018. 04. 10.)

A felkelők ellentámadása és veresége

Április 6-án felújították támadásukat a felkelők. Autóbomba alkalmazásával kezdték a támadást, de csak részleges sikereket értek el.

Újabb támadás következtében a felkelők áttörték a hadsereg Manshiyah kerület nyugati fele köré emelt erődítményét és elfoglalták a teljes kerületet. A Szíriai Hadsereg két nappal később az orosz légierő támogatásával mégis egy ellentámadást indított.

Április 18-án az orosz légierővel megtámogatott szíriai hadsereg ellentámadást indított Manshiyah kerületben, mely során néhány területet megtisztított és visszafoglalt.

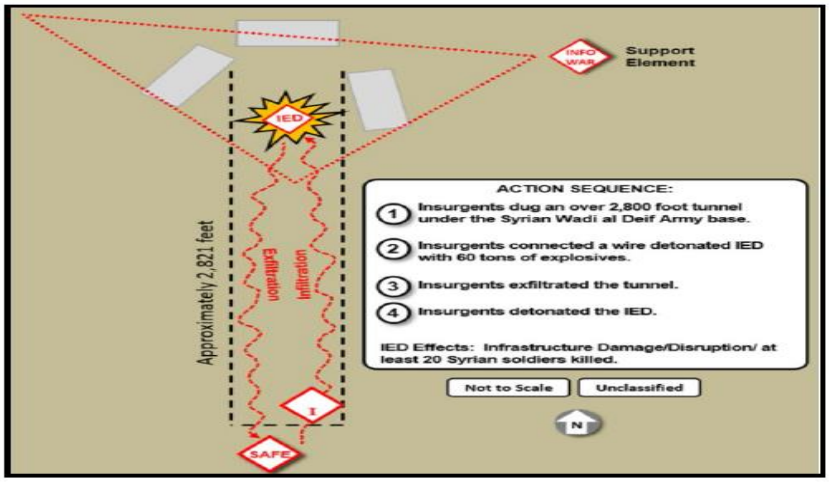
Június 3-án a felkelők egy újabb támadást indítottak Manshiyah területén, de ezt visszaverték. A harcban a két oldalon összesen 31 katona halt meg.[38]

Egyéb esetek, tanulságok, módszerek

Az IÁ elleni harcok katonai tapasztalatai mind az IED támadások, a csapdák és rajtaütések alkalmazásából és a lakott területen folytatott harcokból származnak.

Tekintsük át a tapasztalatokat

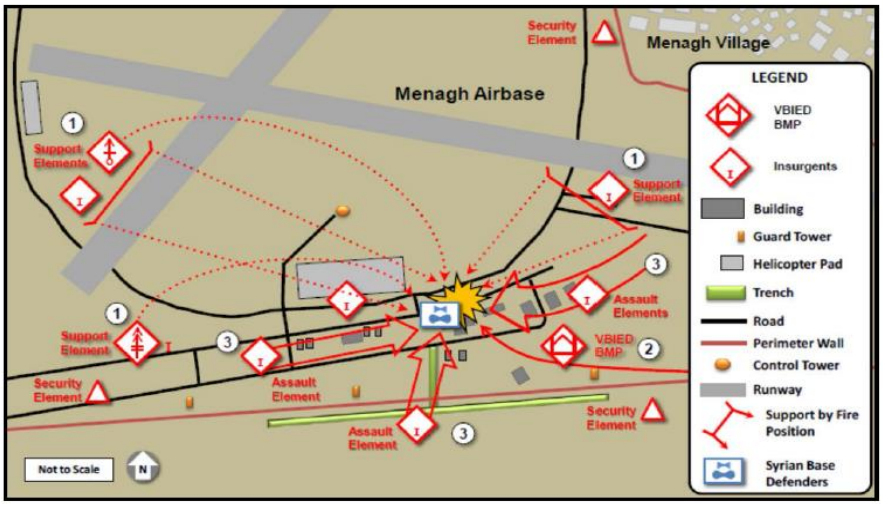
Az egyik fontos katonai harcászati tapasztalat az IED támadásokból adódik. Az IÁ harcosai több alkalommal sikeresen lepték meg az iraki és szíriai kormányerők harc- és gépjármű oszlopait. Az IED-k alkalmazásakor többször „csaliként" IÁ katonák menekülést színleltek, hogy az adott előkészített robbantási helyszínhez csalják az ellenséget. A másik jellemzője volt ezeknek a támadásoknak a több oldalról előkészített, rengeteg robbanóanyagot, fel nem robbant lövedéket, muníciót tartalmazó helyszín. A robbantásokat végig figyelemmel követték, videóra vették, világhálóra jutatták, propaganda céllal, továbbá az ellenség módszereit eljárásait tanulmányozták, hogy a későbbiekben még hatásosabbak legyenek az akcióik.



16. ábra: Wadi al Deif katonai bázis elleni támadás[39]

[38] Syrian Troops Pound Daraa After Rebel Attack, In: https://www.voanews.com/a/syrian-troops-pound-darra-after-rebel-attack/3886454.html (Letöltés ideje: 2018. 04. 10.)

A támadásokat többször sok oldalról indított tűzcsapásokkal, csapatok manőverével együtt alkalmazták. A környező épületek szintjeit felhasználva többlépcsős, tűzcsapásokkal kombinálták a robbantás hatásait. Sokszor a bázisok védelmi építményeinél alagutat ástak, több tonna robbanóanyagot robbantottak, majd a hatásokat kihasználva bejutottak a bázisokra.



17. ábra: A Menaghi légibázis elleni támadás[40]

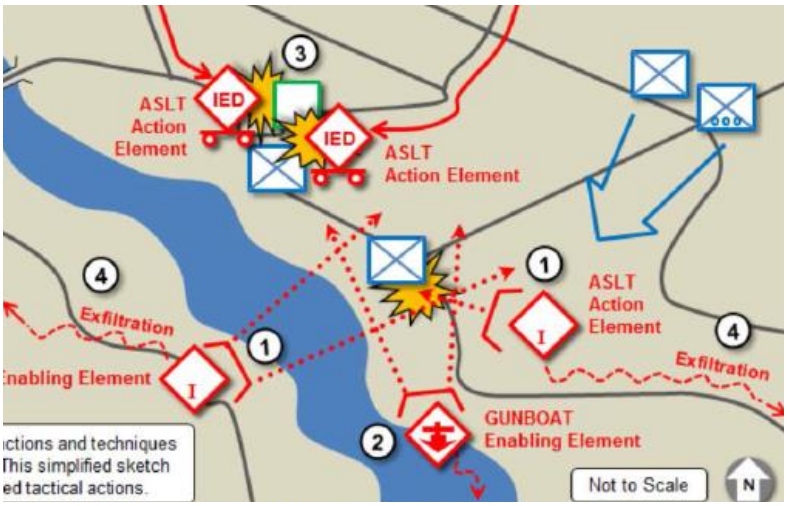
A légi bázis elleni támadást a lövészárkokat elfoglalva, az őrtornyok között behatolva, harcjárművekkel (BMP-1), biztosító és támogató elemekkel együtt hajtották végre. Az IÁ harcosai tűzzsákot képezve tűzzel fenyegették a helikopter felszálló hely biztonságát, továbbá a légi bázis szíriai védőit.

Az IED-s támadásokat sokszor meglepő módon harcjárművekről és kihasználva a sok vízi utat, csónakról és a víz túlpartjáról végrehajtott tűzcsapásokkal kombinálták.

---

[39] Forrás: Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf, p. 9. (Letöltés ideje: 2018. 04. 14.)

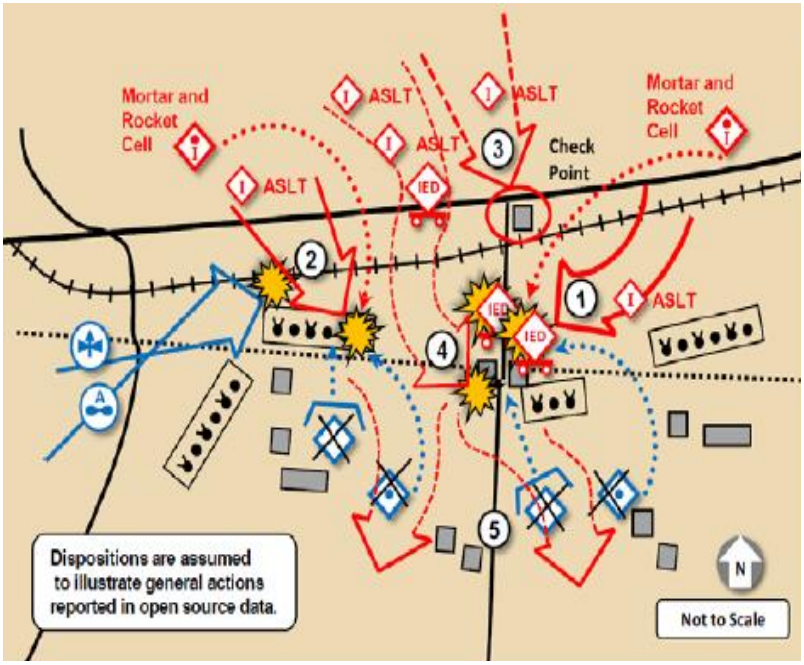
[40] Forrás: Forrás: Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf, p.10. (Letöltés ideje: 2018. 04. 14.)



18. ábra: Géppuskával felszerelt csónakkal elkövetett támadás[41]

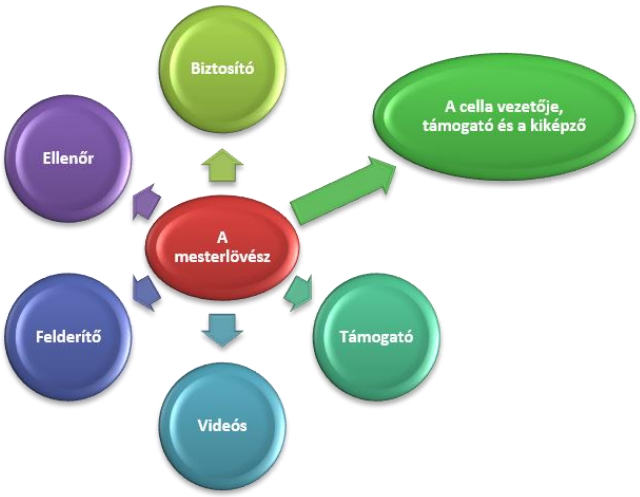
A védelmi létesítmények és támpontok ellen elkövetett támadások egyik kedvelt módszere volt az úgynevezett „TABQA" támadás. Ennek lényege, hogy a támadó alegységek előtt több gépjármű és harcjármű öngyilkos merénylethez került előkészítésre, ők voltak a „faltörő kosok" az ellenség védelmi állásaiba való behatolásnál. A műszaki zárakon áthaladva robbantottak átjárót, majd a csapatok peremvonalába behajtva hajtották végre a robbantásokat. Az ellenséges csapatoknál pánikot idéztek elő. A robbantásos merénylőket második lépcsőként követő alegységek tüzérségi csapások fedezete alatt gyors, lerohanó támadást hajtottak végre. Nagyon gyorsan, 10-15 perc alatt egy ellenséges század katonái által megszállt támpontot fel tudtak számolni.

[41] Forrás: Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf, p. 18. (Letöltés ideje: 2018. 04. 14.)



19. ábra: A TABQA támadás[42]

Mesterlövészek alkalmazásának tapasztalatai



20. ábra: A mesterlövész alkalmazása, segítői[43]

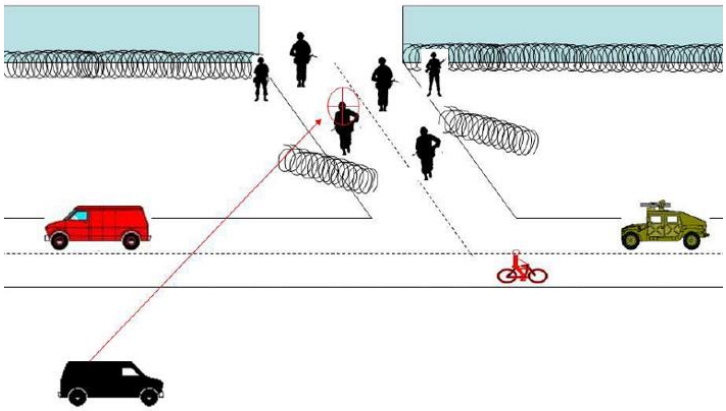
[42] Forrás: Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf, p. 11. (Letöltés ideje: 2018. 04. 14.)

[43] Forrás: IED and Sniper Defeat: The Battle Staff Operations Process in a COIN Environment, In: https://info.publicintelligence.net/USArmy-BattleStaff.pdf, p. 25. (Letöltés ideje: 2018. 04. 14.) Szerkesztette: Dr. Resperger István

A mesterlövészek alkamazásánál a támogatást, a propagandát, továbbá a folyamatos fejlesztést tartották szem előtt az IÁ terroristái. A módszereik közül keiemelkedik:

- gépjárművek átalakítása,
- katonai bázisok körüli alkalmazás,
- ellenőrző-áteresztő pontoknál történő bevetés,
- járőröző katonák, rendőrök elleni alkalmazás,
- gyermekekkel katonai konvojok megállítása, majd tűzcsapása mesterlövészektől,
- komplex alaklamazás, rajtaütéskor, együttműködve más csoportokkal,
- magas építményekről katonai bázisok, irányába,
- IED-vel kombinált támadásokkal együtt.[44]

A járőröző katonák elleni alkalmazásoknál a gépjárműből végrehajtott akcióknál a gépjármű másik gépjármű takarásából készült fel a lövésre. Itt helyezkedett el a mesterlövész, a vezető és az ellenőrző. A kerékpáros személyek a felderítést végezték, más járműből a videósok rögzítették az akciót, majd a gyors menekülés következett.



21. ábra: Járőr elleni mesterlövész alkalmazás[45]

A gyermekekkel együtt történő alkalmazás

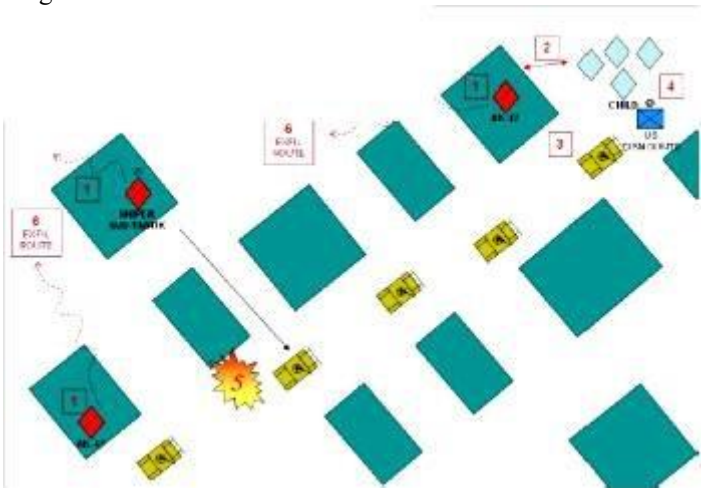
A mesterlövészeket a lakott területen gyakran alakalmazták a bázisokról kivonuló katonai járműoszlopok és menetet végrehajtó alegységek ellen. A gyermekeket a konvoj elé terelték, megállásra kényszerítve a járműveket. A

---

[44] IED and Sniper Defeat: The Battle Staff Operations Process in a COIN Environment, In: https://info.publicintelligence.net/USArmy-BattleStaff.pdf, pp. 24-36. (Letöltés ideje: 2018. 04. 14.)

[45] Forrás: IED and Sniper Defeat: The Battle Staff Operations Process in a COIN Environment, In: https://info.publicintelligence.net/USArmy-BattleStaff.pdf, p. 29. (Letöltés ideje: 2018. 04. 14.)

mesterlövészek az oszlopot oldalról vették tűz alá. Az oszlop elején és a végén történő biztosítást alkalmaztak a szemben levő területekről, a magasabb helyiségek tetejéről pedig az akciót videózták.



22. ábra: Mesterlövész alkalmazása gyermekekkel[46]

A mesterlövészek alkalmazásának nemcsak a fizikai megsemmisítés volt a lényege, hanem a pszichológiai hatás is. A sebesült katonát szeretnék a társai megmenteni, de nem tudnak mindig beavatkozni a jól megválasztott tüzelési szektor miatt. Az információs hadviselés területén pedig a lelőtt katonákról a videófelvételek demorlizálhatták társaikat, illetve az IÁ részére győzelemként lehett a videócsatornákra eljutattni. A katonáik nagyon jó kiképzést kaptak, több hadszíntér tapasztalatait egyesítették, a beépített területek és a városi harc mesterei és kulcsszereplői voltak.

Ha a filmek hatásaira gondolunk, már a II. világháború időszakától a finn mesterlövészek, vagy a legendás Zajcev Sztálingrád védelménél, továbbá a jelenkor híres filmje „Az amerikai mesterlövész" mutatja igazi hatásait.

A győzelem és a stratégia hadtudományi kérdései

„Az ellenség hadseregét le kell győzni, a területét el kell foglalni, és a lakosság akaratát meg kell törni"[47] – ez jellemzi a clausewitz-i szentháromságra épülő győzelmi stratégiát.

A mostani konfliktusok viszont azt mutatják (Líbia, Szíria, Irak, Afganisztán), hogy az ellenség a katonai végállapot elérésére úgy törekszik, hogy elérje a szövetséges erők kivonulásunkat. Céljuk: megtörni és kifárasztani, kivéreztetni a szövetséges erőinket, ehhez az aszimmetrikus hadviselést alkalmazzák.

---

[46] Forrás: IED and Sniper Defeat: The Battle Staff Operations Process in a COIN Environment, In: https://info.publicintelligence.net/USArmy-BattleStaff.pdf (Letöltés ideje: 2018. 04. 14.)

[47] CLAUSEWITZ Carl von: A háborúról, Zrínyi Kiadó, 2014, Budapest, p. 171. ISBN: 9789633275993

Összegzés, az IÁ lakott területen folytatott tevékenységének jellemzői

- kisalegységekre tagolt szervezet (raj, mesterlövész párok);
- a raj szervezetében kézi páncélelhárító rakéta (RPG-7), géppuska, kézifegyverek, kézigránátok, Molotov-koktél is található;
- ritkább esetben kézi légvédelmi rakéta (SZTRELA, esetleg STINGER);
- a rajok folyamatos járőrözést, helyváltoztatást végeznek;
- a csapdára alkalmas helyeken, a falakon lőrések, a tetők, a pincerészek előkészítése;
- rögtönzött házi készítésű robbanóeszközök előkészítése és aknák telepítése;
- vegyi fegyverek alkalmazásának előkészítése;
- drónokkal aknavető gránátok eljuttatása a célok fölé és alkalmazásuk;[48]
- zsákmányolt harcjárművek, polgári járművek átalakítása, páncéllemezekkel történő megerősítése;
- gép- és harcjárművek előkészítése öngyilkos merényletekhez;
- egyéni öngyilkos merénylők felkészítése, technikai előkészítése;
- megerődített kisebb körletek, lakások, házak előkészítése;
- jól megtervezett tüzelési szektorok, tűzösszpontosítási körletek és tűzzónák előkészítése;
- a kisalegységekkel összehangolt manőverek előkészítése, ellenlökés végrehajtása, előkészített tűzszakaszok elfoglalása, tűzcsapások végrehajtása;
- halogató harctevékenységi formák alkalmazása a nem döntő fontosságú körletekben;
- esetenként a civil lakosság élő pajzsa mögötti tevékenység;
- a lakosság ellenállóképességének fenntartása céljából mozgósító és pszichológiai jelleggel beszédek megtartása, a vezető Abu Bakr al-Baghdadi üzeneteinek közvetítése;
- a harci csoportok tevékenységének videón történő rögzítése, a világhálón történő terjesztése;
- célzott és tudatos kivégzések félelemkeltés céljából (elfogott ellenséges katonák, rendőri erők tagjai, illetve a lakosság);
- raktárak, bázisok, lőszer-, üzemanyag-, élelem-, ivóvízkészletek képzése, tárolása;
- kis teljesítményű rádió-adóvevők, mobiltelefonok alkalmazása;
- a hadijog szerint hitszegő cselekmények előkészítése a nemzetközi szervezetek felségjeleinek felhasználásával (Vörös Félhold, Vöröskereszt);
- a médiumok beengedése a megszállt övezetbe, városba propaganda céllal;
- esetenként a média munkatársainak elfogása, kivégzése;
- a nem állami szervezetek munkatársainak elfogása, kivégzése;
- a menekülő lakosság közé terroristák bejuttatása, felderítés, terrorcselekmények végrehajtása céljából;
- túszok szedése és kivégzése.

[48] A Phantom FC40 Quad Copter került sokszor alkalmazásra, melynek ára 50 USA dollár. Forrás: Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf, p. 19. (Letöltés ideje: 2018. 04. 14.)

Mi lehet a szövetségesek stratégiája?

A katonai végállapot megteremtése után a politikai végállapot megvalósítására az eddig tervezett 5-10 éves intervallum sajnos nem elegendő, mert a szétesett államok helyrehozatala még normál társadalmi szinten állók esetén is nehéz, de egy elmaradt térség gondjait rendezni rendkívül szűkös. Ezek mellett a biztonságot kell folyamatosan garantálni, egy időben a humanitárius és a harci feladatok ellátásával. Célunk a biztonság megteremtése, az akaratunk rákényszerítése az ellenségre. Legyőzni és elfogni azt, megtörni, s ehhez modern, hálózatközpontú hadviselést kell használnunk. Korszerű elvek, modern eszközök, gyors győzelem a nyílt hadszíntéren, de rengeteg áldozat saját és polgári oldalon a megszállást követően. Ennek ellenére a műveletek tapasztalatai alapján, ha nem is tudunk egy NATO tervezési rendszerből kiindulva műveleteket tervezni és végrehajtani a GOP (Guidelines for Operational Planning – Hadműveleti Tervezési Útmutató) és COPD (Comprehensive Operations Planning Directive – Átfogó hadműveleti tervezés direktívája) módszerekkel, azok módosított változatát használhatjuk felsőstratégiai, hadműveleti és harcászati tervezésnél. A módosított változat lényege az, hogy ezek az ellenálló és egyéb csoportok nem meghatározható Center of Gravityvel (Súlypont) rendelkeznek, hanem nagyon hatásos részképességekkel, úgymint: felderítés, tűzvezetés, vezetés, kommunikáció és nem utolsó sorban lakossági támogatás. Ezért stratégiánkat a feltartóztatásra és a korlátozásra kell fókuszálnunk. A másik jellegzetesség, hogy nem szakaszokkal, zászlóaljakkal kell küzdenünk, hanem hálózatosan felépített cellákkal, nagyon jól felkésztett katonákkal.

Felderítés területén a biztonság növelése érdekében olyan rendszabályokat kell bevezetnünk, amelyek megnehezítik a saját csapataink, bázisaink, járőr útvonalaink beazonosítását, megközelítését és tűz alá vételét.

Az ellenfél ***mozgékonyságának*** korlátozására a gépkocsik rendszámának távoli felismerhetőségét, továbbá üzemanyag-korlátozást kell bevezetnünk. Minden gépjárműmozgás saját csapataink irányába fenyegetésként kell kezelni, mert módszereik között a gépjárművel elkövetett öngyilkos merényletek nagy számban fordultak elő.

Az ellenség ***vezetését*** a felderítés hatékonyságának növelésével kell korlátoznunk. (Főleg a HUMINT (Human intelligense) – Emberi erőforrással folytatott felderítés, a SIGINT (Signal Intelligence) – Rádiólelektronikai felderítés és UAV-k (Unmanned Vehicle) – Pilótanélküli repülőeszköz kiterjedt alkalmazásával.)

A tűzerő korlátozásánál a védettségünket, a rendszabályok betartását, a személyi felszerelések szabályos viselését és a lehető legrövidebb idő alatti gyors tűzkiváltást biztosító hord-módját kell szem előtt tartanunk. Robbantásos merényletek ellen a kontra IED módszereket kell alkalmaznunk. Ehhez a robbanó eszközökhöz való hozzáférést, begyűjtést és megsemmisítést kell bevetnünk. A csapásoknál előnyben kell részesítenünk a precíziós eljárásokat, főleg pilótanélküli eszközök alkalmazásával.[49]

---

[49] HASKOLOGLU, İsa – EKER, A. Alparslan – ADANA, Şaban: A Perspective of Applications of Unmanned Systems in Asymmetric Warfare, http://www.ijiet.org/papers/356-K3004.pdf (Letöltés ideje: 2015. 11. 14.)

Tervezésnél a biztonság minden dimenziójára figyelemmel meg kell akadályoznunk, hogy az ellenség értékelhető, pontos információkkal rendelkezhessen mozgásunkról, tevékenységünkről, ne alkalmazhasson a támadási körzetünkben, bázisainknál UAV-at.

A lakossági támogatás megszerzése érdekében nem szabad elnyomóként mutatkozni. Fontos és betartandó a vallás, a történelem, a hagyományok tisztelete, így talán lesz civil támogatás. Meghatározó az együttműködés a nemzetközi szervezetekkel és nem állami szervezetekkel.

Befejezés

Az aszimmetrikus konfliktusok egyik jellemzője, hogy a hadszíntér egy hatszög alakú sakktáblán játszódik. Az egyik szereplő az IÁ és támogatói, a kialakult koalíció és támogatói, a nemzetközi szervezetek (ENSZ, EBESZ, EU, Afrikai Unió), a nem állami szervezetek (NGO – Non-Govermental Organisation). A tábla közepén sajnos a belső menekültek a lakosság és a média található. A győzelmet az tudja kivívni, aki nemcsak a katonai győzelmet, hanem az azt követő békét is meg tudja nyerni, jobb állapotokat tud biztosítani a hosszú ideje szenvedő lakosságnak és a menekülteknek.

23. ábra: Az aszimmetrikus hadviselés színtere a hatszög alakú sakktábla[50]

Az Iszlám Állam tervezési módszerei megismerése által levonhatjuk azt a következtetést, hogy egy tervszerűen, hatékonyan felépített, üzemeltetett és minden tervezési szintre (politikai stratégia, katonai stratégia, harcászati módszerek) kiterjedő tevékenységgel álltunk szemben.

Ebben a sok-sok szereplőt, aktív geopolitikai játékost (Egyesült Államok, Oroszországi Föderáció, Szaúd-Arábia, Törökország. Irán) és geopolitikai pillért (Szíria, Afganisztán, Irak) felvonultató történetben a sok nemzetiségi, vallási, etnikai ellentét sokkal élesebb formában befolyásolhatja a konfliktus kimenetelét.

[50] Szerkesztette: RESPERGER István

Felhasznált irodalom:

- ARMSTRONG, Karen: Mohamed (az iszlám nyugati szemmel), Európa, Budapest, 1998. 429. p. ISBN: 9630764245
- BARRETT Richard: The Islamic State, http://soufangroup.com/wp-content/uploads/2014/10/TSG-The-Islamic-State-Nov14.pdf (Letöltés ideje: 2015. 09. 27.)
- BHARDWAJ, Maya: Development of Conflict in Arab Spring Libya and Syria: From Revolution to Civil War, https://pages.wustl.edu/wuir/development-conflict-arab-spring-libya-and-syria-revolution-civil-war (Letöltés ideje: 2015. 09. 27.)
- BRISARD, Jean-Charles – MARTINEZ, Damien: Islamic State: The Economy-Based Terrorist Funding, https://risk.thomsonreuters.com/sites/default/files/GRC0815.pdf, (Letöltés ideje: 2015. 09. 27.)
- CLAUSEWITZ Carl von: A háborúról, Zrínyi Kiadó, 2014, Budapest, p. 171. ISBN: 9789633275993
- DUPUY, R. Ernest – DUPUY N. TREVOR: The Encyclopedy of Military History Harper and Row, Publisher, New York and Evanston 1970. 1406 p. http://mno.hu/kulfold/nem-ker-az-iszlambol-a-britek-tobbsege-1280069 (Letöltés ideje: 2015. 09. 26.)
- FADEL, Leith: Syrian Army turns the tables on the jihadist rebels in Daraa, several points recaptured: video, al-Masdar News, (Letöltés ideje: 2018. 04. 10.)
- FLAMOTHE Dan – GIBBONS-NEFF Thomas – KARKLIS Laris – MEKO Tim: Battle of Mosul: How Iraqi forces defeated the Islamic State, In: https://www.washingtonpost.com/graphics/2017/world/battle-for-mosul/?utm_term=.bd9dab107241 (Letöltés ideje: 2018. 04. 10.)
- HASIM Ahmed, S.: From Al Kaida affiliate to the rise of the Islamic Caliphate: The evolution of the Islamic State of Iraq and Syria (ISIS) RSiS Nanyang Technologial University, 2015.
- HASKOLOGLU, İsa – EKER, A. Alparslan – ADANA, Şaban: A Perspective of Applications of Unmanned Systems in Asymmetric Warfare, http://www.ijiet.org/papers/356-K3004.pdf (Letöltés ideje: 2015. 11. 14.)
- HERRMAN, Rainer: Az Iszlám Állam, A világi állam kudarca az arab világban pp. 30-32. TILGHMAN, Andrew, "The myth of AQI," Washington Monthly, October 2007, retrieved January 26, 2010 from http://www.washingtonmonthly.com/features/2007/0710.tilghman.html (Letöltés ideje: 2015. 09. 20.)
- Military Balance 2015. Szerk.: NEAMAN, Rachel, The Institute for Strategic Studies London, 1996.
- NAPOLEONI, Loretta: Az iszlamista Főnix, Budapest: Hvg könyvek. 2015. ISBN 978-963.304-264-9. 216.p.

- RESPERGER István: Az aszimmetrikus hadviselés Belülről jövő fenyegetések. A „green on blue" (GOB) támadások háttere és az ellenük való védelem előadás az MHTT Aszimmetrikus hadviselés konferenciáján, Budapest, 2014. 11. 12-én.
- RESPERGER István – KIS Álmos Péter – SOMKÚTI Bálint: Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással. Zrínyi Kiadó, 2013. Budapest. 421 p. ISBN: 9789633275924
- ROSTOVÁNYI ZSOLT: Az iszlám a XXI. század küszöbén, Aula, Budapest, 1998. 498. p. ISBN: 9639078581
- ROSTOVÁNYI ZSOLT: Mit kell tudni az iszlámról, Kossuth Könyvkiadó, Budapest, 1983. 239 p. ISBN: 9630923025
- TERRILL, W. Andrew: Special Report: The Islamic State, In: http://www.clarionproject.org/ (Letöltés ideje: 2015. 09. 20.)
- TILGHMAN, Andrew: The myth of AQI," Washington Monthly, October 2007, retrieved January 26, 2010.
- TOMSON, Chris: Modest gains as the Syrian Army continues Daraa counter-offensive, al-Masdar News (Letöltés ideje: 2018. 04. 10.)
- WINTER, Charlie: The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf, pp. 18-21. (Letöltés ideje: 2015. 11. 25.)
- WINTER, Charlie: Women of the Islamic State A manifesto on women by the Al-Khanssaa Brigade, https://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/women-of-the-islamic-state3.pdf (Letöltés ideje: 2015. 09. 27.)
- WILSON, Jeremy – ROSEN, Armin – BENDER Jeremy: These are the weapons Islamic State fighters are using to terrify the Middle East In: https: uk.businessinsider.com/isis-military-equipment-arsenal-2016/#social-media-27 (Letöltés ideje: 2018. 04. 27.)
- YEGINSU, Ceylan: ISIS Draws a Steady Stream of Recruits From Turkey. The New York Times. 15 Sept. 2014. Web. 11 Nov. 2014., http://www.nytimes.com/2014/09/16/world/europe/turkey-is-a-steady-source-of-isis-recruits.html,(Letöltés ideje: 2015. 09. 20.)
- ZAHIYEH, Ehab: How ISIL became a major force ith only a few thousand fighters. June 19, 2014, retrieved June 23, 2014 from http://america.aljazeera.com/articles/2014/6/19/isil-thousands-fighters.html The Economist. (Letöltés ideje: 2015. 09. 20.)

Internetes hivatkozások:

- Analysis: The Battlefield in Syria's Southernmost City, Daraa, In: https://www.newsdeeply.com/syria/articles/2017/06/23/analysis-the-battlefield-in-syrias-southernmost-city-daraa (Letöltés ideje: 2018. 04. 10.)

- COIN Environment, In: https://info.publicintelligence.net/USArmy-BattleStaff.pdf p. 25. (Letöltés ideje: 2018. 04. 14.)
- Country Reports on Terrorism 2011." U.S. Department of State. Published July 31, 2012. http://www.state.gov/j/ct/rls/crt/2011/195553.htm# Accessed August 2, 2012. (Letöltés ideje: 2018. 04. 14.)
- Country Reports on Terrorism," United States Department of State, Office of the Coordinator for Counterterrorism, April 2006, retrieved on February 4. http://www.state.gov/documents/organization/65462.pdf, p. 220. (Letöltés ideje: 2018. 04. 14.)
- IED and Sniper Defeat: The Battle Staff Operations Process in a COIN Environment, In: https://info.publicintelligence.net/USArmy-BattleStaff.pdf, (Letöltés ideje: 2018. 04. 14.)
- Szn.: Country Reports on Terrorism, United States Department of State, Office of the Coordinator for Counterterrorism, April 2006, retrieved on February 4, 2010 from http://www.state.gov/documents/organization/65462.pdf, p. 220. (Letöltés ideje: 2015. 09. 20.)
- Szn.: Country Reports on Terrorism 2011., U.S. Department of State. Published July 31, 2012. http://www.state.gov/j/ct/rls/crt/2011/195553.htm#ig, (Letöltés ideje: 2015. 09. 20.)
- Szn.: Accessed August 2, 2012., {Zahiyeh, Ehab. "How ISIL became a major force ith only a few thousand fighters." June 19, 2014, retrieved June 23, 2014 from http://america.aljazeera.com/articles/2014/6/19/isil-thousands-fighters.html, (Letöltés ideje: 2015. 09. 20.)
- Syrian Troops Pound Daraa After Rebel Attack, In: https://www.voanews.com/a/syrian-troops-pound-darra-after-rebel-attack/3886454.html (Letöltés ideje: 2018. 04. 10.)
- The Economist: The Islamic State of Iraq and Greater Syria: Two Arab counties fall apart, The Economist. June 13, 2014, retrieved June 23, 2014 from http://www.economist.com/news/middle-east-and-africa/21604230-extreme-islamist-group-seeks-create-cal, (Letöltés ideje: 2015. 09. 20.)
- Threat Tactics Report: Islamic State of Iraq and the Levant, In: https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf, p. 17. (Letöltés ideje: 2018. 04. 14.)
- https://www.almasdarnews.com/article/isis-positions-hammered-mosul-families-flee/ (Letöltés ideje: 2018. 04. 14.)
- https://www.almasdarnews.com/article/updated-battle-map-of-daraa-city-southern-front-brigades-on-the-offensive/ (Letöltés ideje: 2018. 04. 10.)
- https://www.almasdarnews.com/article/battle-mosul-enters-day-three-isis-consolidates-frontline-map-update/ (Letöltés ideje: 2018. 04. 10.)
- http://www.bbc.com/news/world-middle-east-37702442 (Letöltés ideje: 2018. 04. 10.)
- http://iswresearch.blogspot.hu/search/label/Iraq (Letöltés ideje: 2018. 04. 10.)

- http://mno.hu/kulfold/nem-ker-az-iszlambol-a-britek-tobbsege-1280069 (Letöltés ideje: 2015. 09. 26.),
- https://moly.hu/konyvek/winston-s-churchill-sohase-engedjetek (Letöltés ideje: 2018. 04. 10.)
- http://www.nytimes.com/2011/04/26/world/middleeast/26syria.html?_r=1&hp (Letöltés ideje: 2018. 04. 10.)
- http://www.nytimes.com/2014/09/16/world/europe/turkey-is-a-steady-source-of-isis-recruits.html (Letöltés ideje: 2015. 09. 26.)
- https://www.rt.com/news/263769-iraq-isis-humvees-weapons/ (Letöltés ideje: 2018. 04. 15.)
- https://southfront.org/iraqi-map-update-battle-for-mosul-on-november-8-2016/ (Letöltés ideje: 2018. 04. 10.)
- http://www.state.gov/documents/organization/65462.pdf, (Letöltés ideje: 2015. 09. 26.)
- https://study.com/academy/lesson/asymmetric-warfare-definition-tactics-examples.html (Letöltés ideje: 2018. 04. 14.)
- https://www.theguardian.com/cities/2018/mar/26/mosul-struggles-recover-ruins-iraq-isis#img-1, (Letöltés ideje: 2018. 04.03.)
- https://www.usatoday.com/story/news/world/2017/05/30/iraq-government-has-yet-decide-if-renew-critical-work/102198756/ (Letöltés ideje: 2018. 04. 14.)
- https://www.washingtonpost.com/world/in-baghdad-us-defense-secretary-to-size-up-iraqi-forces-will-to-fight/2015/07/23/384b284e-30ad-11e5-a879-213078d03dd3_story.html (Letöltés ideje: 2015. 12. 12.)
- http://www.washingtonmonthly.com/features/2007/0710.tilghman.html, (Letöltés ideje: 2015. 09. 26.)

DR. LÁSZLÓ VIKTÓRIA

A BIZTONSÁGOT VESZÉLYEZTETŐ TÉNYEZŐK, AZOK HATÁSAI ÉS KÖVETKEZMÉNYEI NAPJAINKBAN

Bevezetés

A XX. század végén jelentős változások zajlottak világszerte. A Szovjetunió és a szocialista tömb felbomlásával a hidegháború befejeződött és a kétpólusú világrend felbomlott. Számos, a két nagyhatalom – az Amerikai Egyesült Államok és a Szovjetunió –, valamint szövetségeseik által addig kontroll alatt tartott, mélyben megbújó probléma tört a felszínre.

Ezzel párhuzamosan a bipoláris világrend felbomlása kedvező terepet teremtett a globalizáció egyre nagyobb mértékű és egyre több területre begyűrűző térnyerésének. Ennek a folyamatnak a kibontakozásához járult hozzá nagymértékben az óriási léptékekben kibontakozó infokommunikációs forradalom is. A nemzetközi rendszer változásai számos értelmezés, megközelítés, fogalom tartalmának újraértelmezését tették szükségessé az új vagy már korábban is meglévő, de jelentősen átalakult biztonságot veszélyeztető tényezők megjelenésével.

„Az új világrend komplexebb és bizonytalanabb lett”, melynek legfontosabb okai elsősorban a nemzetközi rendszer szereplői számának növekedése, valamint a szereplők nehezebb beazonosíthatósága. Ehhez a változáshoz hozzájárult a globalizáció is, elsősorban a fizikai távolságok szerepének lényeges csökkenésével, a kölcsönös függőségen, egymásra utaltságon és egymásba kapcsolódó érdekhálózatokon alapuló nemzetközi kapcsolatok rendszerével. A világrend változása a biztonság fogalmának és a biztonságot veszélyeztető tényezők jellegének átalakulását is maga után vonta.[1]

A komplexitás és a bizonytalanság tetten érhető a témával foglalkozó tudományos irodalomban is, hiszen egyrészről a biztonság-fogalomnak rendkívüli nagyszámú értelmezése látott napvilágot, másrészről a biztonságot veszélyeztető tényezők száma, elnevezése óriási mértékben nőtt. A különböző tanulmányokban, cikkekben, doktori értekezésekben hasonló tartalommal, szinonimaként a „veszélyek”, „veszélyforrások”, „problémák”, „biztonsági kihívások”, „új típusú biztonsági kihívások”, „kockázatok”, „kockázati tényezők”, „fenyegetések”, „biztonságot veszélyeztető tényezők”, ”negatívan ható jelenségek”, a „biztonságra negatívan ható tényezők” elnevezés egyaránt használatos, ezen a téren sem beszélhetünk egységes, letisztult fogalomhasználatról.

[1] RADA Péter: Átalakuló biztonsági kihívások. A biztonság dimenziói, Grotius. Forrás: http://www.grotius.hu/doc/pub/KZQSCF/rada%20p%C3%A9ter%20%C3%A1talakul%C3%B3%20biztons%C3%A1gi%20kih%C3%ADv%C3%A1sok.pdf, p. 1. (Letöltés ideje: 2018. 03. 05.)

A biztonság fogalmának kibővülése, annak értelmezése

A hidegháború idején a biztonság fogalma alatt elsősorban a nemzetállamok nemzeti biztonságát értették, melynek központi elemét az egyes államok fenyegetésekkel szembeni katonai képessége jelentette. A biztonságot a fenyegetések hiányaként vagy a fenyegetésekre való reagálás képességeként értelmezték.

Az utóbbi évtizedekben a nemzetközi biztonság fogalma egyre komplexebbé vált, amely szükségessé teszi a fogalom szélesebb és átfogóbb megközelítését. A korábbi katonai fogalmakkal és tartalmakkal bíró, territoriális értelemben vett nemzeti biztonság fogalmával szemben a biztonság nem katonai dimenziójának megnövekedett jelentősége figyelhető meg. Észlelhető „… *a politikai, szociális, gazdasági, ökológiai és humán kockázatok felzárkózása a katonai kihívások mellé".* A problémát tovább árnyalja, hogy a kihívások gyakran egyidejűleg jelentkeznek.[2]

A biztonság-fogalom bővítésének szándéka összeforrt Barry Buzan nevével, aki az általa vezetett koppenhágai iskola kutatóival kidolgozta a szektorelméletet. Az elmélet a biztonság addig elfogadott katonai dimenzióján kívül további négy területtel - a politikai, gazdasági, társadalmi, környezeti szektorral - bővítette a fogalom értelmezését.

„A biztonság fogalmának kibővülése nem ért véget a bipoláris világrend eltűnésével, ahogy a nemzetközi rendszer változásai sem fejeződtek be. A bővülés egyszerre jelentkezik vertikális és horizontális síkon." Vertikális értelemben a bővülés Buzan szektorelmélete alapján a katonai dimenzión kívül a politikai, gazdasági, társadalmi, környezeti dimenzióban figyelhető meg.

A horizontális bővülés a nemzetközi élet szereplői - a multinacionális vállalatok, a pénzügyi intézmények, a nemzetközi szervezetek, a nem kormányzati szervezetek - számának növekedésében érhető tetten.[3]

A biztonságot veszélyeztető tényezők csoportosítása

A biztonságot veszélyeztető tényezők számos csoportosítása ismert. A kategorizálás alapja lehet, hogy ezeket a tényezőket mely szereplők – állami vagy nem állami szereplők – tevékenysége idézi elő, a biztonság mely szektorában éreztetik hatásukat, kit/kiket veszélyeztetnek. Elterjedt és az egyik leginkább elfogadott csoportosítási mód az eredet/ származás, a méret, a hatókör, valamint a fokozat/intenzitás szerinti felosztás.

---

[2] GAZDAG Ferenc – TÁLAS Péter: A biztonságot veszélyeztető tényezőkről I. (2008.) Forrás: http://www.nemzetesbiztonsag.hu/cikkek/gazdag_ferenc__talas_peter-a_biztonsagot_veszelyeztet___tenyez__kr__l_i_.pdf, pp. 3-4. (Letöltés ideje: 2018. 03. 11.)

[3] GAZDAG Ferenc: A biztonságpolitikai kihívások természetéről (2012.) Forrás: http://www.grotius.hu/doc/pub/CEKOFW/2012_35_gazdag_a_biztonsagpolitikai_kihivasok_termeszeterol.pdf, p. 14. (Letöltés ideje: 2018. 03. 05.)

Fokozat/intenzitás alapján a bonyolultabb, súlyosabb irányba mutató sorrendiség alapján a biztonságot veszélyeztető tényezők lehetnek: kihívások, kockázatok, fenyegetések, válságok, konfliktusok és háborúk.[4]

A kihívások, a kockázatok és a fenyegetések a lehetséges veszélyek megnyilvánulási formáinak tekinthetők, „*…amelyek általában hátrányosan befolyásolják a belső és a külső stabilitást, és hatással lehetnek egy adott régió hatalmi viszonyaira. Ezek a fogalmak egymásra épülve egyre nagyobb feszültségi szint meglétét feltételezik. Jellegükből következően csak dinamikus folyamatokként értelmezhetőek. Ezért a fogalmi meghatározások az elméleti értelmezés szempontjából fontosak, de a gyakorlatban gyakran egymást átfedve, összemosódva jelennek meg, és a külső környezeti jellemzők (például a politikai és a gazdasági viszonyok) függvényében képlékenyen változhatnak. Értékelésük és elemzésük nem ritkán csak egy újabb stabilizálódott erőtér kialakulása után, visszamenőleg végezhető el*.” A kockázatok és a kihívások szintjén leginkább a környezeti és a gazdasági elemekre, míg a fenyegetések szintjén alapvetően a politikai, a diplomáciai és a katonai elemekre helyeződik a hangsúly.

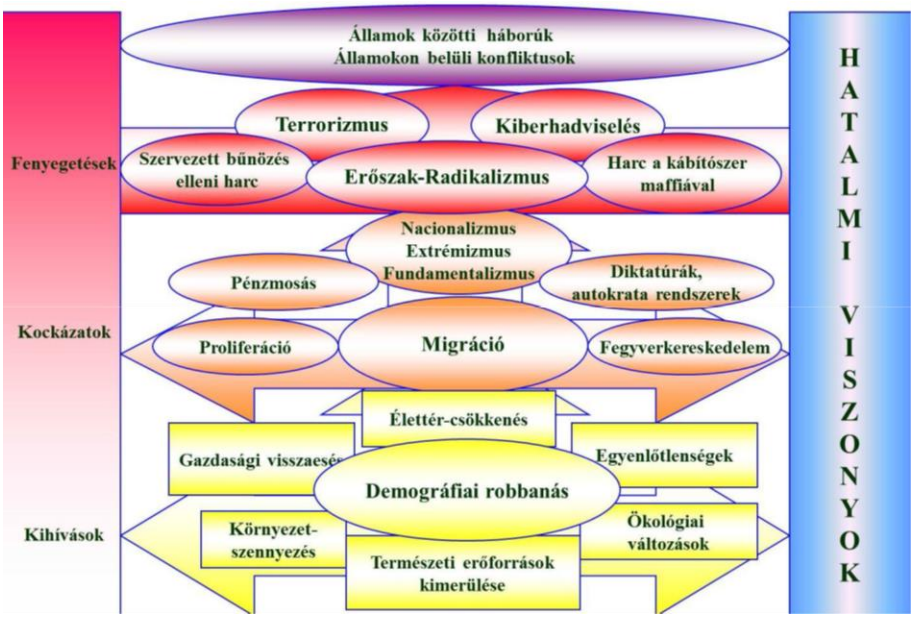
A „kihívások”, „kockázatok”, „fenyegetések” meghatározások alatt valamennyi olyan helyzetet és állapotot értünk, amelyek az általánosan értelmezett biztonság egyes összetevőire hatnak. Ezek a hatások a kihívások esetében a lehetséges veszélyek legalacsonyabb megnyilvánulási szintjén érezhetők, a kockázatok esetében azon a megnyilvánulási szinten, „*… amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek”*, míg a fenyegetések esetében a legmagasabb megnyilvánulási szinten jelennek meg a hatások, amikor a nemzeti érdekek sérülhetnek, és közvetve hatással lehetnek a nemzeti értékek megőrzésére.[5] A fenyegetések körében előtérbe kerül az érdekek képviseletének lehetséges módszerei és eszközei között a kikényszerítés vagy az erőszakos úton történő megoldás lehetősége.[6]

---

4 Uo. pp. 6-10.

5 RESPERGER István (2013): Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig. Felderítő Szemle, XII. évf. 3. sz. Forrás: http://www.knbsz.gov.hu/hu/letoltes/fsz/2013-3.pdf, pp. 5-6. (Letöltés ideje: 2018. 03. 12.)

6 RESPERGER István: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során. Doktori (PhD) értekezés. Forrás: http://docplayer.hu/5999686-A-fegyveres-erok-megvaltozott-feladatai-a-katonai-jellegu-fegyveres-valsagok-kezelese-soran.html, p. 36. (Letöltés ideje: 2018. 05. 15.)



1. ábra: Kihívások, kockázatok és fenyegetések[7]

A másik, igen gyakran használt kategorizálás alapja, hogy a biztonságot veszélyeztető tényezők a biztonság mely szektorában – katonai, politikai, gazdasági, társadalmi, környezeti – jelentkeznek.

A különböző csoportosítások vizsgálatával összefüggésben azonban megállapítható, hogy az egyes szektorokban jelentkező tényezők esetén nem húzható éles határvonal, egyes szektorok között átfedések vannak. Megállapítható továbbá az is, hogy az egyes szektorokban negatívan ható tényezők többsége megújult formában és intenzitással jelentkezik, gyakran több tényező egy időben, mindezek folytán súlyosabb következményeket okozva. A biztonságot veszélyeztető tényezők egymással összekapcsolódnak, kölcsönhatásban vannak, gyakran erősítik egymás hatását, továbbá lokális problémát okozva könnyen válhatnak regionális vagy globális jelentőségűvé.

Napjaink globális biztonsági kihívásai, kockázatai és fenyegetései

Az egyik legnagyobb, globális szinten jelentkező kihívás ***a bolygó népességének növekedése***. Ez a folyamat Afrikához és Dél-Ázsiához köthető, míg Európában a népesség fogyatkozik.[8]

---

[7] Forrás: RESPERGER István: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során. Doktori (PhD) értekezés. Forrás: http://docplayer.hu/5999686-A-fegyveres-erok-megvaltozott-feladatai-a-katonai-jellegu-fegyveres-valsagok-kezelese-soran.html, p. 136. (2018.05.15.)

[8] RESPERGER (2013) p. 10.

A népességnövekedés együtt jár a városok számának és méretének növekedésével, ugyanakkor a kiapadóban lévő forrásokért – ivóvíz, energia – folytatott küzdelem kiéleződésével, valamint a növekvő környezetszennyezéssel és környezeti terheléssel. Egyre nagyobb számú ember nem jut megfelelő minőségű és mennyiségű ivóvízhez, valamint egyre kevesebb víz marad a mezőgazdaságnak, ami – a hiányos infrastruktúrával, valamint az elosztási problémákkal együttesen – a fejlődő országokban egyre kevesebb élelmiszer biztosításához, ezáltal egyre nagyobb mértékű éhínséghez vezet. Ezt a folyamatot a klímaváltozás tovább erősíti.

Ezen tényezőkön kívül a gazdaság további globalizációja, a jövedelmi különbségek – szegény-gazdag régiók között, államok között, államokon belül – növekedése, a szétesett államhatalmak, elhúzódó háborúk, az állandósult vallási, faji, törzsi konfliktusok is embertömegeket késztetnek migrációra.[9]

A népességnövekedéssel együtt járó ipari és mezőgazdasági vízfogyasztás növekedése, valamint a klímaváltozás negatív következményei hatására „*…2025-ben 2,4-3,4 milliárd ember fog ún."vízstresszes" országokban élni",* elsősorban az afrikai, közel-keleti, dél-ázsiai országokban, valamint Észak-Kínában.[10]

A növekvő számú embertömeg ellátása maga után vonja a termelés- és a termelékenység növelésének kényszerét, amely nagymértékben megnöveli az energiaigényt, azonban a klasszikus energiahordozók ebben vagy legkésőbb a következő évszázadban kimerülnek. A globális energiaigény növekedése – amelynek növekedési ütemét az erősen fejlődő Kína és India tovább erősíti –, a kiapadóban lévő energiaforrások egyenlőtlen előfordulása, valamint az a körülmény, hogy a lelőhelyek és a szállítási útvonalak nagy része instabil régiókban és államokban van, növeli az erőforrásokat egyre nagyobb mértékben igénylő fejlett világ - így Magyarország - kiszolgáltatottságát.[11]

A stratégiai nyersanyagokból – kőolaj, földgáz – rendelkezésre álló véges készletek problémája maga után vonja a fogyasztó fejlett országok függésének fokozódásán túl a termelő országok piaci erejének, valamint a szállítás biztonságának garantálásában kulcsszerepet játszó tranzit országok szerepének növekedését. Az energiaellátás biztonsága, mint a gazdasági szektorban jelentkező egyik legfontosabb kihívás, „*… az a jelenség, amely mind rövid és hosszú távon a legélesebben megmutatja a globális egymásra utaltságot, vagyis, hogy politikai, katonai vagy gazdasági szempontból erős államok sem érezhetik magukat biztonságban, hiszen kiszolgáltatottak a termelőknek, akik általában kicsi és gyenge intézményekkel rendelkező államok."*[12]

A globális biztonsági kockázatok között kiemelendő a ***migráció*** kérdése. A népességnövekedés – melynek döntő többségét a fejletlen országok adják –, a jövedelmi különbségek növekedése, a katasztrófák, az ivóvíz- és az élelmiszerhiány,

---

[9] BENEDEK Márta: A nemzetbiztonság stratégiai kérdései a XXI. század kül- és biztonságpolitikájában. Doktori (PhD) értekezés. Forrás: http://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10874/Teljes%20sz%c3%b6veg%21?sequence=1&isAllowed=y, pp. 53-59. (Letöltés ideje: 2018.03.18.)

[10] RESPERGER István (2013) i. m. p. 18.

[11] GAZDAG (2012) i. m. pp. 10-11.

[12] RADA i. m. pp. 7-8.

az elhúzódó konfliktusok, az egyes államok működésképtelenné válása és ezzel párhuzamosan a terrorszervezetek és a szervezett bűnözés térnyerése következtében hatalmas embertömegek kényszerülnek elhagyni otthonaikat. A fentebb felsorolt tényezők többnyire összekapcsolódva, egymás hatását erősítve jelentkeznek, melyek tovább súlyosbítják az érintett lakosság helyzetét.

„…a migráció több mint 150 millió embert érint világszerte…. A migráció tovább globalizálódik: egyre több országot fognak érinteni a migrációs mozgások.[13] *A migráció, legyen az legális vagy illegális, társadalmi, biztonsági és nemzetbiztonsági kulcskérdéssé vált, mivel biztonságpolitikai kockázatokat rejt a befogadó ország összes alrendszere számára."* A szakemberek egy része a migráció – illetve a bevándorlók leszármazottai – és a terrorizmus közötti összefüggést hangsúlyozza.

„A befogadó államokban nő az idegengyűlölet, megerősödnek a befogadó migránspolitika ellen nyíltan fellépő pártok,"[14] a nemzetállamoktól eltérő értékrenddel, gyakran eltérő jogrenddel bíró párhuzamos társadalmak jönnek létre jellemzően a nagyvárosokban és elővárosaikban, ahol döntően bevándorlók és leszármazottaik élnek. A migráció negatív hatásai között emlegetik a bevándorlóktól való félelem megjelenését és fokozódását, a bevándorlók beilleszkedési nehézségeiből, az integráció elutasításából fakadó problémákat, továbbá azt, hogy feszültséget generál a szociális ellátó rendszerekben.

A globális szinten jelentkező biztonsági fenyegetések közül talán az egyik legfontosabb a ***globális éghajlatváltozás***, hiszen ezen tényező következményei a bolygón minden embert közvetlenül érintenek már ma is. A környezetpusztulás, a biológiai sokféleség csökkenése, az esőerdők pusztulása, az ózonréteg károsodása, az üvegházhatás, a levegő-, víz-, talajszennyezés növekedése és ezek következményeiként az egyre gyakrabban és intenzívebben szélsőségessé váló időjárás, az elsivatagosodás, az árvizek általános jelenségekké váltak. Az időjárás okozta természeti katasztrófák egyre gyakoribbak és egyre nagyobb pusztítást végeznek.

Az utóbbi időben a tudományos világban egyre inkább felerősödtek azok a hangok, melyek szerint a természettel való „békés együttélésben" elkéstünk, egyes természeti folyamatok – elsősorban a klímaváltozással kapcsolatos jelenségek – irányíthatatlanná váltak, önálló életet élnek, túlléptek a megfordíthatósági küszöbön. A környezeti problémák kezelésének egyik legnagyobb akadálya, hogy hatásaik rövid távon nem feltétlenül jelentkeznek. A másik akadály, hogy gyakran nem azonos a probléma okozója annak károsultjával.[15]

A globális felmelegedés felgyorsulásának jövőbeli következményei beláthatatlanok, amelynek számos negatív következménye között megjelenik az ivóvízhiány, a mezőgazdasági termelékenység csökkenése, a trópusi betegségek északabbra tolódása, az emberek egészségére gyakorolt romboló hatás, valamint az egyes államok működésképtelenné válásának fokozása, elősegítése. Mindezek a

---

13 RESPERGER István (2013) p. 20.
14 BENEDEK i. m. p. 60.
15 GAZDAG (2012) i. m. pp. 34-35.

következmények az államok közötti és államokon belüli feszültségeket növelik, konfliktusok forrásává válnak. Egyéb, biztonságot veszélyeztető tényezőkkel – etnikai, vallási feszültségekkel – együttesen fegyveres konfliktusok kialakulásához vezethetnek. A leginkább veszélyeztetett régiók a túlnépesedett, elmaradott régiók, főként Észak-Afrikában, a Közel-Keleten és Dél-kelet Ázsiában.[16]

A ***terrorizmus*** az egyik – sajnálatos módon – legaktuálisabb és leginkább közismert biztonsági fenyegetés napjainkban. A hidegháborút követően „új arcát mutató" terrorizmus kialakulásában a globalizáció óriási mértékű hatása, valamint a hidegháborút követően kiéleződött vallási, etnikai és államokon belüli konfliktusok játszották a főszerepet. Fő célpontokká az Amerikai Egyesült Államok és szövetségesei katonai, diplomáciai kirendeltségei, érdekeltségei és állampolgárai váltak.[17] A céljait, ideológiai alapjait, célpontjait, szervezeti felépítését, finanszírozását, elkövetési eszközeit, módszereit tekintve megváltozott terrorista hálózatok legnagyobb veszélyét lélektani előnyük adja. A cél a félelemkeltés a nyilvánosság és a médiaszereplés felhasználásával, egy-egy állam destabilizálása, kormányának „megalázása", *„az állandó pszichológiai hadviselés ébrentartása".*

Főként vallási, politikai, etnikai, személyes indíttatásból, döntően civilek ellen nagyvárosokban, izoláltan követnek el merényleteket egyes kisebb terrorista csoportok, sejtek, valamint mind gyakrabban magányos elkövetők. *„Ezek az „önradikalizálódó egyének" gyakran egyetlen hálózatnak sem tagjai, csak ideológiai közösségben érzik magukat valamelyikkel, és úgy hajtják végre akcióikat, hogy a magszervezetnek nincs is tudomása róla. Terepük és színterük az Internet."*[18] Az egyes hálózatok többnyire önfinanszírozók, forrásaik javarészt csalásokból, kiadványok értékesítéséből, tagdíjak, adók beszedéséből, különböző adománygyűjtő kampányokból, a zsarolóvírusok segítségével a felhasználóktól származó váltságdíjakból származnak.

A terrorakciók előkészítése és végrehajtása ma már modern technikai eszközök és nagyobb hatásfokú robbanószerkezetek felhasználásával történik. *„Reális a veszélye továbbá annak is, hogy a terrorcsoportok tömegpusztító fegyverekhez, vegyi és biológiai fegyverekhez juthatnak és ezeket fel is használják, valamint ún. piszkos bombát gyártanak."*[19] A tényleges veszélyt a biológiai, kémiai, radiológiai fegyverek terrorcsoportok általi megszerzése és felhasználása jelenti, hiszen az előállításukhoz szükséges technológia, szakértelem, valamint a felhasznált anyagok - duális hasznosíthatóságuk révén - megtalálhatók a civil életben.[20]

Századunk másik fontos biztonsági fenyegetése a ***szervezett bűnözés.*** Ezen a területen is nagymértékű átalakulások figyelhetők meg. Sokkal intenzívebb a nemzetközi hálózatokba, szövetségekbe tömörülésük, tevékenységi körük nemzetközi szintűre történő kiterjesztése. Tevékenységükből származó óriási tőkéjüket a legális gazdaságba forgatják vissza, befolyásolásuk iránya ezen túl egyre inkább a központi és helyi államigazgatás, igazságszolgáltatás, kulturális területek és a média irányába terelődik. Jellemzői a professzionális szakemberek, új ágazatok

16 RADA i. m. pp. 9-11.
17 RESPERGER István (2013) p. 28.
18 BENEDEK i. m. p. 62.
19 Uo. pp. 60-66.
20 RADA i. m. pp. 4-5.

megjelenése – személyazonosság ellopása, online zsarolás, számítógép hackelés –, jelenleg formálódó, új típusú szervezett bűnözői kör kialakulása, működési hatékonyságuk növekedése, a terrorizmussal való egyre nagyobb összefonódás.

A szervezett bűnözés és a terrorizmus erősödését segíti a technológia fejlődése, az információs hálózatok széles körű kiépülése is. Kiemelendő jelenség a terrorizmus és a szervezett bűnözés egyre nagyobb mértékű szervezett összefonódása. A terrorista szervezetek a szervezett bűnözői csoportok módszereit alkalmazva juttatják be tagjaikat a célországokba, segítségükkel jutnak hozzá az akciók elkövetéséhez szükséges eszközökhöz, a nemzetközi szervezett bűnözés nyújtotta lehetőségek kiaknázásával[21] – főként a kábítószer-kereskedelemből – biztosítják anyagi forrásaik egy részét. Az együttműködés alapvetően technikai okokra vezethető vissza. Egymás „szolgáltatásait" használva érdekkapcsolatok jönnek létre, eltérő céljaik eléréséhez alkalmazott módszereik egyre inkább megegyeznek. A terrorizmus és a szervezett bűnözés összefonódásának kedvező „táptalajt" biztosítanak olyan tényezők, mint a társadalmon belül növekvő jövedelmi különbségek, a túlzsúfolt városok, a működésképtelenné váló államok, az etnikai, vallási törésvonalak mentén mélyen megosztott társadalom.[22]

Az informatikai, információs kihívások és a kiberterrorizmus a biztonságot veszélyeztető tényezők között talán a legintenzívebben fejlődő, újabb és újabb területeken felbukkanó negatívan ható tényező. Ennek legfőbb oka, hogy a fizikai valóság és a kibertér egyre inkább összekapcsolódik. A fizikai valóságban megvalósuló tevékenység államhatárokat átlépve, a kibertérbe is kiterjeszkedik és fordítva. A kibertérben megjelenő veszélyek, támadások és azok következményei a fizikai világban is éreztetik hatásukat. „… *az információs hálózatok széleskörű kiépülése, amely állami eszközökkel nem szabályozható, lehetővé teszi a szervezett bűnözés és a terrorizmus térhódítását, a védett rendszerekbe való bejutást, a pénzügyi, az államigazgatási és a katonai rendszerek megcsapolását, illetve rombolását."*[23]

A kiberterrorizmus egyik megvalósulási módja, amikor a célpont az informatikai rendszer, míg a másik esetben az informatikai rendszer az elkövetés eszköze, melynek segítségével más típusú bűncselekményeket követnek el. A cél egyes hálózatok ellehetetlenítése, valamilyen információ megszerzése, figyelemfelhívás vagy közvetlen anyagi haszonszerzés.[24]

Magyarország vonatkozásában a globális biztonságot veszélyeztető tényezőkkel – különösen a migráció, az éghajlatváltozás és a kiberterrorizmus – azok globális jellege folytán, valamint azok negatív következményeivel számolnunk kell.

Az utóbbi években Európára rázúduló ***migráció***s áradat hazánkat is jelentősen érintette. Magyarország tipikusan a tranzit országok közé sorolható, azonban nem

---

[21] BENEDEK i. m. pp. 66-71.

[22] RADA i. m. p. 5.

[23] LAKATOS Zsolt: Transznacionális veszélyek, fenyegetések – és a katonai hírszerzés. Felderítő Szemle 2018/K p. 14. Forrás: http://www.knbsz.gov.hu/hu/letoltes/fsz/2008-konferencia.pdf (Letöltés ideje: 2018.03.05.)

[24] BENEDEK i. m. pp. 71-72.

zárható ki annak a lehetősége, hogy a jövőben egyes csoportok számára célországgá válik.

Magyarországra a ***terrorizmus*** kapcsán jelenleg a leginkább jellemző a „tranzit-lét", azonban egy estlegesen bekövetkező terrorista támadással[25] főként hazánk nemzetközi szerepvállalása kapcsán számolnunk kell.

A ***szervezett bűnözés*** alapvetően hazánkban homogén, nemzeti jellegű, a hagyományos bűnözés – kábítószer-, árucsempészet, gazdasági bűnözés – terén fejti ki tevékenységét, alapvetően fiktív társaságok útján.[26]

A ***demográfiai változások*** Magyarországon a népesség számának fokozatos csökkenésével, annak fokozódó ütemű elöregedésével, valamint a szakképzett munkaerő országból történő elvándorlásával jellemezhetők. „*Egyrészt a korosztályi struktúra változása – a gazdaságilag aktív és passzív lakosok arányának változása miatt – negatívan hat az ország jövedelemtermelő képességére, másrészt a kiadási oldal (nyugdíj- és egészségügyi ellátás) nagyobb terhei a költségvetésre rónak fokozott terheket".*[27] Az elvándorlás szintén – a kieső bevételek folytán – a szociális ellátó rendszerek túlterheléséhez, munkaerőhiányhoz, ezáltal a gazdaság termelékenységének csökkenéséhez vezet. Mindezek a folyamatok társadalmi, politikai feszültségeket generálnak.

A globális ***éghajlatváltozás*** hatásai hazánkban is érezhetők az egyre gyakoribbá váló hirtelen lezúduló nagy mennyiségű csapadék, az aszályos időszakok hosszának növekedése, az egyre gyakrabban előforduló és egyre nagyobb hőmérsékleti ingadozások formájában. Vízrajzi adottságai miatt kiszolgáltatott a szomszédos országokból (Ausztria, Románia) a folyókon keresztül érkező környezeti szennyezéseknek. A környezeti biztonságra az ár- és belvizek, az aszályok, a viharok, a környezet- és légszennyezés, valamint az illegális hulladéklerakás jelentenek leginkább veszélyt.[28] „*A jövőben egyre gyakrabban kell számolni súlyos következményekkel járó környezeti katasztrófákkal és közegészségügyi válsághelyzetekkel."*[29]

A kiberterrorizmus körében elkövetett cselekmények nem ismernek államhatárokat, így Magyarország, a magyar társadalom és a gazdaság veszélyeztetettségét is fokozzák, legyen szó vírusterjesztésről, adatlopásról, dezinformáció terjesztéséről, valamint bármely „egyszerű" kiberbűnözés vagy akár idegen titkosszolgálati információszerzés keretében megvalósuló tevékenységről.

---

[25] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról 1. melléklet 29. pont. Forrás: http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf. (Letöltés ideje: 2018.05.15.)

[26] GAZDAG (2012) i. m. p. 25.

[27] TÓTH Rudolf: A lakosságvédelem aktualitása, helye, szerepe napjaink új kihívásainak tükrében. pp. 63. Polgári Védelmi Szemle 2009/2. Forrás: http://www.mpvsz.hu/letoltes/pvszemle/pv2009_2.pdf, pp. 55-73. (Letöltés ideje: 2018.04.20.)

[28] GAZDAG (2008) i. m. p. 10.

[29] TÓTH i. m. pp. 55-73.

Kibertámadás[30] elsősorban az ország vezetési, politikai, gazdasági, közigazgatási rendszerét, infrastruktúráját, bankrendszerét, a védelmi szférát sodorhatja veszélybe, rövid időn belül óriási károkat okozva.

Összegzés

A fentebb ismertetett szakirodalom elemzése alapján elmondható, hogy számos forrás – publikáció, dokumentum, doktori értekezés – más-más megközelítésben, különböző hangsúllyal és összefüggésekben vizsgálja a napjaink biztonságát veszélyeztető tényezőket. Összességében megállapítható, hogy ezeknek a tényezőknek jelentős része már korábban is létezett, de megjelenési formájuk, előfordulási gyakoriságuk, intenzitásuk megváltozott az utóbbi évtizedekben. A globalizáció folytán gyakran egymással összekapcsolódva, egymás hatásait erősítve jelennek meg, államhatárokat átlépve kiszámíthatatlan, előre nem látható, dominó hatásszerű folyamatokat indítanak, indíthatnak el.

A biztonságra negatívan ható tényezők megváltozott volta, következményeik összetettebbé és előre nem láthatóvá válása az ellenük való védekezést, a kialakuló kockázatokra való felkészülést is jelentősen megnehezíti. A konkrét, rendkívüli helyzetek a hatékonyság érdekében azonnali reagálást tesznek szükségessé. A megváltozott követelményrendszerrel összefüggésben egyre gyakrabban emlegetett vélemények szerint a lehetséges válaszok kialakításánál alapvető fontosságú kiindulási pont lehet a „nem a klasszikus nemzetállami" keretek között, hanem regionális szinten, illetve kétoldalú vagy multilaterális keretek között megvalósuló szoros, folyamatos együttműködés, és ezen belül a gyors információáramlás, az információcsere, a közös információszerzés.

Mindezek a változások másfajta gondolkodásmódot, komplex megközelítést követelnek meg szerte a világban, így Magyarországon is a védelmi rendszerek és a védelmi igazgatás szereplőitől. Megítélésem szerint szükség van Magyarországon a közigazgatás részét képező[31] védelmi igazgatás – valamint az annak szervezeti elemeiként működő megyei és helyi védelmi bizottságok – vonatkozásában is a „mit" és „hogyan" kérdések megválaszolásához annak mélyreható és széleskörű vizsgálatára, hogy a hazai védelmi igazgatás mennyire képes megfelelni a biztonságra negatívan ható tényezők által támasztott új és folyamatosan változó követelményeknek.

Felhasznált irodalom:

- BAÁN Mihály et al. (2014): Magyarország védelmi igazgatása a közigazgatás új környezetében. Budapest, Zrínyi Kiadó

[30] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról 1. melléklet 31. pont. http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf (2018.05.15.)

[31] BAÁN Mihály et al. (2014): Magyarország védelmi igazgatása a közigazgatás új környezetében. Budapest, Zrínyi Kiadó.

- BENEDEK Márta: A nemzetbiztonság stratégiai kérdései a XXI. század kül- és biztonságpolitikájában. Doktori (PhD) értekezés. pp. 272. Forrás: http://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10874/Teljes%20sz%c3%b6veg%21?sequence=1&isAllowed=y (Letöltés ideje: 2018. 03. 18.)
- GAZDAG Ferenc: A biztonságpolitikai kihívások természetéről. (2012) pp. 1-35. Forrás: http://www.grotius.hu/doc/pub/CEKOFW/2012_35_gazdag_a_biztonsagpolitikai_kihivasok_termeszeterol.pdf (Letöltés ideje: 2018. 03. 05.)
- GAZDAG Ferenc: A biztonságot veszélyeztető tényezőkről III. (2008) pp. 3-18. Forrás: http://www.nemzetesbiztonsag.hu/cikkek/gazdag_ferenc-a_biztonsagot_veszelyeztet___tenyez__kr__l_iii_.pdf (Letöltés ideje: 2018. 03. 12.)
- GAZDAG Ferenc – TÁLAS Péter: A biztonságot veszélyeztető tényezőkről I. (2008) pp. 3-12. Forrás: http://www.nemzetesbiztonsag.hu/cikkek/gazdag_ferenc__talas_peter-a_biztonsagot_veszelyeztet___tenyez__kr__l_i_.pdf (Letöltés ideje: 2018. 03. 11.)
- LAKATOS Zsolt: Transznacionális veszélyek, fenyegetések – és a katonai hírszerzés. Felderítő Szemle 2018/K
- RESPERGER István (2013): Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig. Felderítő Szemle, XII. évf. 3. sz. pp. 5-34. Forrás: http://www.knbsz.gov.hu/hu/letoltes/fsz/2013-3.pdf (Letöltés ideje: 2018. 03. 12.)
- RESPERGER István: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során. Doktori (PhD) értekezés. pp. 275. Forrás: http://docplayer.hu/5999686-A-fegyveres-erok-megvaltozott-feladatai-a-katonai-jellegu-fegyveres-valsagok-kezelese-soran.html (Letöltés ideje: 2018. 05. 15.)
- RADA Péter: Átalakuló biztonsági kihívások. A biztonság dimenziói. Grotius. pp. 1-13. Forrás:http://www.grotius.hu/doc/pub/KZQSCF/rada%20p%C3%A9ter%20%C3%A1talakul%C3%B3%20biztons%C3%A1gi%20kih%C3%ADv%C3%A1sok.pdf (Letöltés ideje: 2018. 03. 05.)
- TÓTH Rudolf: A lakosságvédelem aktualitása, helye, szerepe napjaink új kihívásainak tükrében. Polgári Védelmi Szemle 2009/2. pp. 55-73. Forrás: http://www.mpvsz.hu/letoltes/pvszemle/pv2009_2.pdf (Letöltés ideje: 2018. 04. 20.)
- 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról 1. melléklet 30. pont. Forrás: http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf (Letöltés ideje: 2018. 05. 15.)

BARTÓK ANDRÁS

A KÍNAI NÉPKÖZTÁRSASÁG VÉDELEMPOLITIKÁJA 1989-TŐL NAPJAINKIG

A Kínai Népköztársaság katonai képességeinek drasztikus növekedése a Deng Xiaoping[1] „reform és nyitás" politikájának kiteljesedése óta élénken foglalkoztatja a biztonsági tanulmányok és más diszciplínák gondolkodóit. Kína valós katonai képességét azonban sok esetben szinte misztikus bizonytalanság övezi. Mindez talán nagyban köszönhető annak, hogy a Kínát a modernizáció új szakaszán elindító vezető, Deng, a hidegháború bipoláris rendjének végéhez közeledve határozott iránymutatást adott az ország külpolitikai profiljának alacsony szinten tartására. Ahogyan a Kínai Kommunista Párt (KKP) idézi a nagy reformer megannyiszor elhangzott gondolatmenetét, Kínának a bonyolódó nemzetközi környezetben elsősorban „*nyugalmasan [kell] figyelnie, biztos pozícióba helyezkedni, nyugalommal kezelni a helyzetet, elrejteni erőnket, visszafogott kiállást felvenni, semmiképp sem vezető szerepbe kerülni*".[2]

Ennek köszönhetően Kína katonai ereje sokszor ellentmondásosan jelenik meg az elmúlt három évtized szakirodalmában, hol felfújt, elmaradott hatalomként, hol szinte legyőzhetetlen, a jövő globális erőegyensúlyát hamarosan uraló katonai szuperhatalomként hivatkoznak rá. Jelen tanulmány célja, hogy olyan átfogó képet adjon az elmúlt harminc év fejlődéstörténetéről, amely segít egy folyamat kontextusában szemlélni a Kínai Népköztársaság (KNK) erejének és a Kínai Népi Felszabadító Hadsereg (KNFH) képességeinek eddigi alakulását, és ezzel járul hozzá, hogy pontosabb képet kaphassunk a jövőbeli kilátásokról. Ennek alapjául a fegyveres erők állományának alakulása, főbb fegyverrendszerei, azok növekedését és modernizációját nyomon követő adathalmaz elkészítése szolgált, amely remélhetőleg a jövőben további folyamatos felülvizsgálatok segítségével állandóan naprakész képet tud majd adni a KNK fegyveres erőinek főbb paramétereiről.

Kína nemzetközi befolyásának növekedése széles körben foglalkoztatja a vonatkozó szakirodalom szerzőit mind nemzetközi, mind hazai szinten. Peking katonai stratégiájának értelmezése önmagában is nehéz kihívás elé állítja a kritikus szemléletű megközelítést,[3] annak regionális és az Egyesült Államokkal szembeni érdekütközései, illetve a két hatalom közötti erőegyensúly felmérése pedig további elemzési erőfeszítések alapjait képezik.[4]

---

1 Jelen tanulmányban a szárazföldi kínai szavak átírásakor a kínai nyelv latinbetűs Pinyin rendszerét használom, kivéve azokban az esetekben, ahol a korábbi átírással írt változat már jobban elterjedt a magyar helyesírásban.

2 CPCNEWS: **冷静**观察、沉着应付、韬光养晦、决不当头、有所作为. Forrás: theory.people.com.cn (Letöltés ideje: 2018. 08. 12.)

3 Kínai katonai stratégiájáról bővebben lásd: HÁDA Béla: Útban egy nemzeti álom felé? – Kína 2015. évi katonai stratégiája. Nemzet és Biztonság 2015/9. pp. 125-133.

4 VÖRÖS Zoltán: Kína külpolitikai irányváltása a regionális tengerek vonatkozásában. In. Szakmai Szemle 2014/1. pp. 116-118.

Jelen tanulmány kereteit ugyan meghaladná a kérdéskörrel foglalkozó szakirodalom maradéktalan áttekintése, de némi elemzői egyszerűsítéssel élve a KNK hatalmi potenciáljának növekedése kapcsán két nagyon fontos gondolatmenetet azonosíthatunk, s az általuk felvetett kérdésekre igyekszik válaszolni egy-egy tanulmány:

a. A KNK katonai erejének növekedése és az USA érdekeivel szembeni ütközések természetszerűen elvezetnek-e egy katonai konfrontációhoz a két hatalom között?
b. A KNK politikai berendezkedések sajátosságai hosszú távon a belső feszültségek kiélezésével gátat szabnak-e Kína globális hatalmi pozíciójának?

Az első kérdés kapcsán jól felépített érvelést találhatunk mind a konfrontáció lehetőségét elvető, mind az annak kockázatát előrevetítő álláspontok mentén. A konfrontáció esélyét csekélyebbnek értékelő álláspontok jelentős része koncentrál a Kína és Amerika közötti konfliktus lehetősége kapcsán arra a felvetésre, hogy egy valódi összeütközés egyik félnek sem áll érdekében,[5] többek között például a globális gazdasági folyamatok egyre jobban egymásra utalt természete miatt. A kölcsönös függésre építő megközelítések gyakran hangsúlyozzák Kína gazdasági sikereinek kötődését a békés regionális viszonyok adta stabilitáshoz, leszögezve, hogy felbomlása élesen ütközne Kína érdekeivel.[6] A konfrontáció mellett állást foglaló értelmezések ezzel szemben – rendszerint – a realista perspektívák zéróösszegű játszma megközelítésére építenek. A realista gondolatmenet alapján a kínai-amerikai összeütközést legplasztikusabban John Mearsheimer vezeti le, szerinte ugyanis Kína hatalmának növekedésével természetszerűen kénytelen lesz majd megpróbálni kiszorítani az Egyesült Államokat a régióból, utóbbi azonban nem engedheti meg ennek bekövetkeztét, így nem lesz más lehetősége, mint konfrontálódni a feltörekvő ázsiai hatalommal.[7]

A második kérdés lényegében azt igyekszik felderíteni, hogy Kína belső társadalmi folyamatai nem vezetnek-e el olyan feszültségekhez, amelyek kikezdhetik a Kínai Kommunista Párt kontrollját és így a belpolitikai krízis vethet véget Kína globális hatalommá válásának. Mindezt többek között építik azon folyamatra, hogy a gazdasági reformok adta középosztály-növekedés komolyabb politikai átalakulás nélkül belső feszültségekhez vezet,[8] illetve hogy az elmúlt évek gazdaságtörténeti folyamatai olyan társadalmi egyenlőtlenségekhez vezettek, amelyek hosszú távon komoly kihívás elé állíthatják a KKP-t.[9] A szakértők szerint Kína számára az elkövetkező évek legnagyobb kihívását nem a külső biztonsági

---

5 VÖRÖS i. m. pp. 118-120.

6 ACHARYA, Amitav: Thinking theoretically about Asian IR. International relations of Asia, 2014, in. SHAMBAUGH, David – YYHUDA, Michael (ed.): International relations of Asia. Rowman & Littlefield, 2014.: 59-89., p. 70.

7 MEARSHEIMER, John J.: The tragedy of great power politics. WW Norton & Company, 2001. p. 409.

8 FISHER, Richard D.: China's military modernization: building for regional and global reach. Greenwood Publishing Group, 2008. pp. 4-5.

9 LIU, Guoli: China rising: Chinese foreign policy in a changing world. Palgrave Macmillan, 2016. pp. 194-195.

környezet jelenti, sokkal inkább az, hogy a változó társadalmi folyamatok közepette képes-e „jó kormányzással" kezelni a belső feszültségeket.[10]

A katonai reformok és haderőfejlesztés elsősorban a KNK külső konfrontációs kérdéskörében segíthet árnyalni az összképet. A tanulmány következő szakaszában folyamatában áttekintem a haderőfejlesztés fő fókuszait az elmúlt évtizedekben. Elöljáróban érdemes annyit megjegyezni, hogy a legfontosabb védelmi koncepciók lépcsőzetes egymásra épülése ez idáig sokkal inkább a KNK-fenyegetettség percepciójának csökkentését szolgálta. Ennek első lépése volt a haderő általános korszerűsítésének megkezdése, a Tajvan szigetével szembeni elrettentési képességek kiépítése – főként a sziget elszakadáspárti politikai folyamataira válaszul –, a tengeri irányból érkező fenyegetéssel szembeni elrettentés növelése és végül Kína geopolitikai kihívásainak orvoslása a tengeri erőkivetítési képességek bővítésével. A folyamat logikus folytatása lehet Kína globális katonai erőkivetítési képességeinek kiépítése és növelése, de ennek egyelőre komolyabb logisztikai és geopolitikai korlátai vannak.

A tanulmány további részében először is a védelempolitika és haderő korszerűsítésének összképe szempontjából legfontosabb mérföldkövek áttekintése, a védelmi költségvetése és a KNFH állományának változásaira vonatkozó áttekintő szakasz olvasható. Ezt követi az egyes haderőnemek részletesebb áttekintése. A három hagyományos haderőnem, a KNFH Szárazföldi Haderő, Haditengerészet és Légierő mellett említésre kerülnek a Hadászati Rakétaerők és a Logisztikai Támogató Haderő. Előbbi 2016-ban vált önálló haderőnemmé, korábban az egyesített vezérkar közvetlen felügyelete alá tartozó Hadászati Rakétacsapatok – nem önálló haderőnemi szintként – leginkább „Második Tüzérség" néven voltak ismertek a nemzetközi és hazai szakirodalomban. Utóbbi, a Logisztikai Támogató Haderő szintén 2016-ban jött létre széles palettájú feladatkörrel, ám egyelőre viszonylag kevés információ áll rendelkezésre erről a legfiatalabb haderőnemről.

A táblázatokhoz és grafikonokhoz felhasznált adatok forrásául elsősorban az *International Institute for Strategic Studies* (IISS) által évente elkészített Military Balance évkönyvek vonatkozó fejezetei szolgáltak, összevetve további elérhető forrásokkal. Noha nem lehetünk bizonyosak abban, hogy minden egyes eszköz esetében pontos darabszámot takarnak az adatok, az elmúlt harminc év statisztikai összefüggései alapján viszonylag megbízható forrásanyag áll rendelkezésre. Szerkesztési és terjedelmi megfontolásokból bizonyos ábrák és táblázatok esetén néhány év került kiemelésre, nem minden esetben évenkénti bontásban láthatóak az adatok, itt általában azon szakaszok maradtak ki, ahol nem tapasztalható szignifikáns változás.

A Kínai Népköztársaság védelempolitikai reformjai Mao halálától napjainkig

Kína számára a Mao utáni politikai váltás adott lehetőséget a Kulturális Forradalom évei alatt kialakult káosz orvoslására. A KNFH számára a Kulturális Forradalom kettős hatással járt. Egyrészt, ahogyan az ország más szektoraiban is, a külföldi szakértelemmel szembeni gyanakvásnak és a tisztogatásoknak

[10] SAICH, Tony: Governance and politics of China. Palgrave Macmillan, 2010. pp. 368-369.

köszönhetően jelentősen megakadt a technológiai fejlődés a haderőn belül is[11]. A kutatási és fejlesztési tevékenység ellehetetlenítésével Kína hadereje komoly lemaradásba került a haditechnika terén. Másrészt a KNFH komoly szerepet vállalt a politikai zűrzavar enyhítésében és az ország kritikus szektorainak megőrzésében és működtetésében. A fegyveres erő Kínában több helyen is átvette az állami közigazgatástól a különböző infrastruktúrák megóvásának és működtetésének feladatát, valami jelentős szerepet vállalt a mezőgazdasági szektorban is.[12] A kulturális forradalom összeségében hozzájárult ahhoz, hogy a Mao halálát követő reform és nyitás korszakát a KNFH jelentős technológiai lemaradással, az ennek orvosolására szükséges források és politikai akarat hiányában kezdte, valamint más országok fegyveres erőihez képest jóval több nem hagyományosan katonai tevékenységet végzett. Ez utóbbi egészen a '90-es évek végéig jellemző maradt és a KKP vezetése csak fokozatosan volt képes a haderő nem katonai tevékenységének leépítésére.

Deng Xiaoping 1978-as hatalomra kerülését követően központi alakjává vált Kína átfogó felzárkózásának az elmúlt évtizedek lemaradásához képest. Fő politikai programja a „*Négy Modernizáció*" üzenete köré épült, melynek négy oszlopa az ipar, az agrárszektor, a tudomány és technológia, illetve a haderő korszerűsítése volt.[13] Bár a hivatalos beszédek és a vezetés részéről elhangzó retorika szerint ezen négy szektor fejlesztése szervesen összefügg egymással, a gyakorlatban a legkisebb prioritást a haderő modernizációja élvezte.[14] Mindez megmutatkozott többek között a védelmi költségvetés GDP arányát tekintve alacsony szintjében, illetve a védelmi kiadások reálértékének fokozatos csökkenésében, egészen a nyolcvanas évek végéig. Kína védelmi költségvetése a ma ismert drasztikusan emelkedő tendencián lényegében 1989 után tudott elindulni, javarészt a Négy Modernizáció három másik szegmense és különösen az agrárszektor termelte eredményeknek köszönhetően.[15]

A védelmi kiadások kapcsán a hivatalosan közölt kínai adatokhoz képest a különböző nemzetközi kutatóintézetek és különösen az amerikai védelmi szféra szakértői között általánosan elfogadott alapvetés, hogy a KNK a hivatalosnál jóval többet költ védelmi célokra. Ezen feltételezések mögött több tényező is húzódik, de a legfontosabbak között érdemes említeni az alábbiakat:[16]

- a hivatalos védelmi kiadások feltételezhetően nem tartalmazzák a kutatási és fejlesztési célokra fordított forrásokat;
- további forrást jelent – bár mára már valószínűleg elenyésző – azon bevételek összessége, amelyek a KNFH nem védelmi tevékenysége, hanem üzleti érdekeltségei kapcsán merülnek fel;

---

11 GHOSH, S. K.: China's Military Modernization Programme. China Report, 1978, 14.4: 66-77. p. 74.

12 EILAND, Michael D: Military Modernization and China's Economy. Asian Survey, 1977, 17.12: 1143-1157. pp. 1148-1149.

13 LIN, Chong-Pin: Chinese military modernization: perceptions, progress, and prospects. Security Studies, 1994, 3.4: 718-753. p. 721.

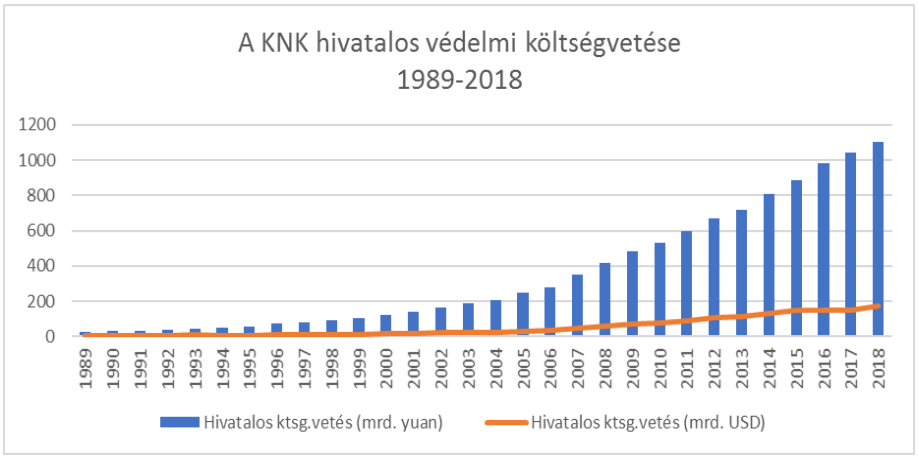
14 SHAMBAUGH, David L.: China's quest for military modernization. Asian Affairs: An American Review, 1979, 6.5: 295-309., p. 302.

15 LIN i. m. p. 724.

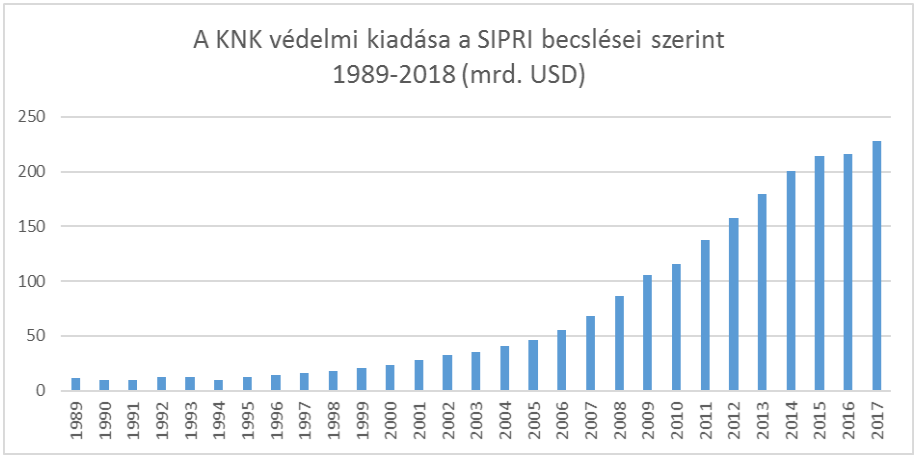
16 IISS: Military Balance 2006. p. 250.

- a hivatalos összeg – feltételezhetően – nem tartalmazta jelentős külföldi, high-end technológiai eszközbeszerzések kiadásait;
- Kína az elmúlt harminc évben komoly fegyverexportőr volt, különösen a harmadik világ országaiba, ám ennek összege nem kerül bele a hivatalos büdzsébe.

Ennek megfelelően érdemes megvizsgálnunk a kínai részről hivatalosan elismert védelmi költségvetést és a különböző nemzetközi kutatóintézetek kritikai megközelítésen alapuló becslését. A KNK védelmi kiadásait – hivatalos kínai adatok szerint – az alábbi grafikonokon tudjuk követni:[17]



1. ábra

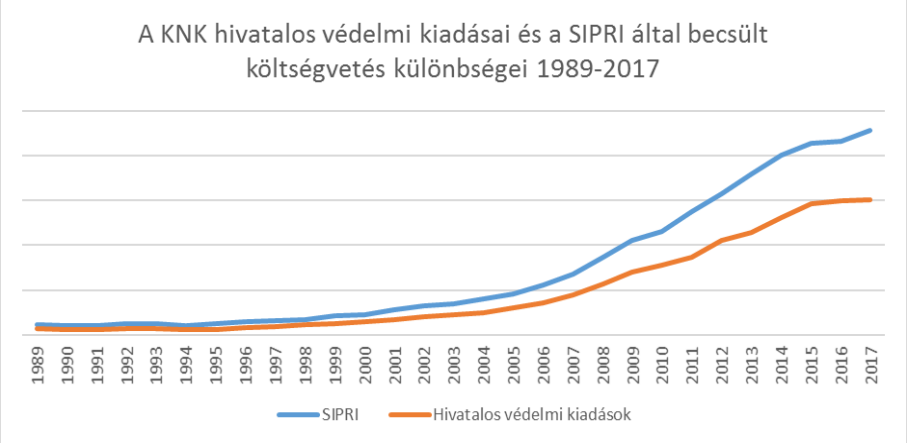


2. ábra

[17] A publikáció ábráinak forrásául az IISS: Military Balance évkönyvek 1989-2018-as számai szolgáltak.

A kínai védelmi költségvetés tényleges nagyságához azonban általában a *Stockholm International Peace Research Institute* (SIPRI) becsült adatait szokás használni, amely jellemzően magasabb, mint a hivatalos kínai adat, de alacsonyabb, mint a Pentagon által közölt és valószínűleg túlbecsült érték.

Érdemes összevetnünk, arányaiban mennyire térnek el a hivatalos költségvetés adatai a SIPRI által becsült, feltehetően a valós védelmi kiadásokhoz közelebb álló értékektől.



3. ábra[18]

Habár nehéz pontosan meghatározni a KNK védelmi kiadásait, az mindenesetre látszik – mind a hivatalos adatok, mind a becsült értékek tükrében –, hogy a védelmi szféra a Deng Xiaoping hatalomra kerülését követő évtizedekben, a kezdeti költségcsökkentéshez képest, 1989 után rendkívüli forrásnövekedést tudhat maga mögött.

A védelmi kiadások növekedése jól mutatja a KNK haderőfejlesztésének ütemét, ám feltehetően ebben több olyan tényező is közrejátszik, ami inkább a fegyveres erők szerepkörének optimalizálást célozták, így a közelebbi kép érdekében érdemes néhány pillantást vetnünk a haderő legfontosabb változásaira is.

Noha a fegyveres erők 1989-ben végre elkezdhette érezni a reformpolitikával járó gazdasági fejlődés előnyeit, a hazai és külföldi politikai események egy darabig még jelentősen hátráltatták a technológiai fejlődést. 1989. június 4-én, a Tienanmen téren történtek után a nyugati országok minden védelmi célú exportot leállítottak Kínába és megszüntettek minden magas rangú katonai látogatást. Kína haderejének modernizációja ezzel veszített lendületéből. A KNK ekkorra komoly exportőrré vált a védelmi a piacon, melynek célországai főként Irán, illetve más közel-keleti országok, például Irak és Szaud-Arábia voltak. Miután új lendületet vett a kínai-szovjet politikai enyhülés, Gorbacsov Pekingbe látogatott, és kilátásba helyezte a

[18] Forrás: Stockholm International Peace Research Institute: SIPRI Military Expenditure Database https://www.sipri.org/databases/milex (Letöltés ideje: 2018. 08. 12.)

kínai határon állomásozó erők csökkentését és a határviták rendezését.[19] A kilencvenes évek első fele látványos közeledést jelentett a kínai-orosz viszonyban. Az enyhülés keretében négy fordulóban zajlottak tárgyalások a határmenti katonai feszültségek enyhítéséről. 1991-ben Moszkva több határfolyón található szigetet adott vissza Kínának. Peking ekkor jelezte érdeklődését szovjet fegyverrendszerek beszerzése iránt, első körben Szu-27-es vadászgépeket vásárolt Moszkvától.[20]

A KNK számára a bipoláris világrend felbomlását követő új korszakban egyik első kihívásként jelentkezett stratégiai elrettentési képességeinek lemaradása. A hadászati rakétaerőinek eszközparkja ekkora már jelentősen elavult, különösen a DF-5 interkontinentális ballisztikus rakéta (ICBM), melynek fokozatos kivonása megkezdődött, a helyébe lépő típus azonban még néhány évig nem volt ismert.[21] Szintén korszerűtlen volt a kínai flotta, a KNFH haditengerészetének korszerűtlen állományát ezért eleinte igyekeztek csökkenteni.

A KNFH Deng alatt fokozatos létszámcsökkentésen esett át. A legnagyobb volumenű valószínűleg 1978-85 között zajlott,[22] ám erről biztosabb adat nem áll rendelkezésre. A haderő szerepe a Tienanmen téren történt esetek rendezésében jelentősen növelte annak politikai profilját, mely egyes források szerint hozzájárult a védelmi kiadások növekedéséhez, de valószínűbb, hogy a ’89 utáni kezdeti években inkább a kínai fegyverexport növekedésének volt köszönhető a védelmi költségvetés növekedése.[23]

Kína hazai fejlesztésű hadiiparán is megmutatkoztak a lemaradás jelei. Ballisztikus rakétahordozó tengeralattjáró-programjának keretében készült második *Xia* osztályú tengeralattjáróját végül nem volt képes hadrendbe állítani és inkább egy új típus fejlesztésébe kezdett.[24] Az egy darab hadrendbe állított egység a későbbiekben főként part menti járőrözési feladatokat volt csak képes ellátni.

A kilencvenes évek elejének fontos mérföldköve volt Kína atomprogramjának utolsó fejlesztési hulláma. Az Átfogó Atomcsend Szerződés (Comprehensive Test Ban Treaty – CTBT) előkészítésének közepette Kína újabb atomkísérletek sorát hajtotta végre – valószínűleg annak érdekében, hogy még a szerződés életbe lépése előtt befejezhesse az ehhez fűződő fejlesztéseket. 1993. október 5-én, egy vélhetően 50-100 kilotonnás erősségű töltetett robbantott, 1994. június 10-én pedig egy10-60 kilotonnás erősségűt. Az eltérő erősségre alapozva, vélhetően új robbanófejek és ezekhez kötődő technológia tesztjeiről lehetett szó.

1994. október 7-én egy újabb, feltehetően 40-150 kilotonnás, 1995. május 15-én pedig szintén egy 40-150 kilotonnás atomtöltet kísérleti robbantását hajtották végre, 1995. augusztus 17-én pedig egy vélhetően 20-80 KT erősségűt. 1995 júniusában rakétakísérletre került sor, vélhetően a DF-31 prototípusával. Ezzel az

---

19 IISS: Military Balance 1989. p. 145.
20 IISS: Military Balance 1991. p. 149.
21 IISS: Military Balance 1989. p. 145.
22 IISS: Military Balance 1991. p. 148.
23 IISS: Military Balance 1989. pp. 145-146.
24 Uo.

USA nyugati partvidéke és Európa egésze bekerült a kínai ballisztikus rakéták hatótávolságába.[25]

Az 1995-96 közötti időszakban került sor a tajvani krízis incidenseire. A sziget elszakadáspárti politikai diskurzusa ugyanis felélénkült az 1996-ban rendezett első közvetlen demokratikus elnökválasztás közeledtével. A KNK aggodalommal figyelte a korábban enyhülőben lévő kapcsolatrendszert, tartva attól, hogy jelentősen megnő az elszakadáspárti politikai erő a szigeten, ezért minden lehetséges eszközzel igyekezett nyomást gyakorolni Tajvan közéletére. 1995 júliusában a KNK nagyszabású haditengerészeti gyakorlatot tartott a sziget közelében, melynek keretében két napon keresztül ballisztikus rakétákat lőtt át a sziget fölött.[26] Feltehetően a Tajvannal kapcsolatos incidensekkel összefüggésben, a KNFH Hadászati Rakétacsapainak kötelékében hadrendbe állított ballisztikus rakéták számát növelték, főként a közepes- és rövid hatótávolságú eszközökét.[27]

A tajvani krízis dinamikája nem csak a szárazföldi Kína és a sziget viszonyában hozott változásokat, de hatására az Egyesült Államok is növelte védelmi elköteleződését ázsiai szövetségesei felé. A kínai hadgyakorlatra és ballisztikus rakétakísérletekre válaszul egy amerikai repülőgép-hordozó harccsoport haladt át a Tajvani-szoroson. Az USA továbbá megerősítette együttműködéseit más regionális szövetségeseivel, megújították az amerikai-japán szövetség irányelveit és új lendületet kapott az ANZUS védelempolitikája. Az amerikai védelmi elköteleződés megerősítésének Kína mellett Észak-Korea állt a középpontjában.[28]

Kína 1996. július 29-én hajtotta végre utolsó kísérleti atomrobbantását. Ezt követően a KNK bejelentette a moratóriumot a további atomkísérletek kapcsán és elköteleződését a CTBT-hez.

1996-ban fontos mérföldkőnek számít a KNK hadiiparának fejlődése szempontjából a korszerűbb vadászgépek hazai gyártásának kezdete. Kína gyártási licenszet kapott a Szu-27 vadászgéphez Oroszországtól, az akkori tervek szerint 150 db eszköz kínai gyártására. A kínai-orosz kapcsolatok elmélyedésének jeleként 1996 áprilisában Jiang Zemin és Borisz Jelcin bejelentették, hogy a két ország stratégiai partnerséget kötött.[29]

A reformfolyamatok és a haderőfejlesztés ellenére a KNFH továbbra is leginkább területvédelmi feladatokra berendezkedett haderő volt, érdemben inkább létszám és mennyiségi alapon képviselt súlyt, mint technológia terén. Kína erőkivetítési képességeit továbbra is gyengének értékelték. Ekkor még nem állt rendelkezésre jelentős nehézfegyver- és csapatszállítási képesség, illetve a KNFH Haditengerészetének felszíni egységei relatíve gyenge légvédelmi és tengeralattjáró-elleni hadviselési kapacitással rendelkeztek.

Kína 1998-ban adott ki először védelmi fehér könyvet, melyben Tajvan egyesítése kapcsán a békés megoldás mellett kötelezte el magát, de fenntartotta

---

25 IISS: Military Balance 1995. p. 170.
26 IISS: Military Balance 1995. pp. 171-172.
27 Uo. p. 176.
28 IISS: Military Balance 1996. p. 170.
29 Uo. p. 171.

magának a jogot szükség esetén akár ezt fegyveres erővel is véghezvigye.[30] A szakértők szerint azonban Kínának ekkor még nem álltak rendelkezésre egy Tajvan elleni partraszállás végrehajtására valódi kapacitásai.[31]

A kilencvenes évek végéhez közeledve a kínai hadiipar függése a közvetlen külföldi – főleg orosz – beszerzésektől kezdett kiegészülni hazai haditechnikai fejlesztésekkel. Ezt jól illusztrálja az első önálló fejlesztésű vadászgép, az F-10, illetve J-10 néven ismert típus első prototípusának tesztrepülése 1998 márciusában.[32] Ám a hazai fejlesztések mellett továbbra is számottevő orosz eredetű fegyvert importált a KNFH, 1999-ben döntöttek például a Szu-30-as vadászgéptípus beszerzéséről.[33]

Az ezredfordulóhoz érve Kína védelempolitikai reformjai és haderőfejlesztési erőfeszítései az 1989-es állapotokhoz képest jelentős előrelépéseket értek el, ám összességében a KNK katonai erejének változásai ekkor még érdemben nem változtattak a regionális erőviszonyokon. A feltételezések szerint Kína számára Tajvan kapcsán egyre reálisabb opcióvá vált a sziget tengeri szállítási útvonalainak elvágása, de egy sikeres partraszállás 2000-ben még kívül esett a KNFH kapacitásain. Tajvan számára leginkább aggasztó tényező a KNK ballisztikusrakétákra építő elrettentési képessége, az ezredfordulón valószínűleg 200-300 rakéta sorakozott a szigetországgal szemben.[34]

Folytatva a személyi állomány csökkentését, a KNFH 1999-2001 között jelentősen csökkentette a sorkatonai állományt a haderőn belül, 85%-ról 65%-ra.[35] Emellett a fejlesztésekben kiemelt figyelmet évezett a tengeri védelem kérdése. 2001-ben megkezdődött egy új hadászati ballisztikusrakétahordozó atomtengeralattjáró fejlesztése, Type 094 néven.[36]

2004-re már a KNFH mindegyik haderőnemén meglátszott az általános eszközmodernizáció és elavult eszközpark kivezetése mellett nagyobb lendületet vett az információs technológiák integrációjának támogatása. Vélhetően ekkor kezdődött meg a *Vezetés, Irányítás, Kommunikáció, Számítógép, Hírszerzés, Megfigyelés és Felderítés* (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* – C4ISR) rendszerek jelentős fejlesztése és az ilyen irányú beruházások dinamikus növelése.

Hu Jintao elnök szimbolikusan a legfelsőbb politikai vezetés részéről is jelezte az elköteleződést a haderő korszerűsítése iránt – kiemelt figyelmet szentelve a ballisztikus rakéta egységeknek –, amikor ígéretet tett a tudományos és technológiai reformok növelésére, miszerint: *„…a stratégiai rakétaelhárítás létrehozása és a*

---

30 Information Office of the State Council Of the People's Republic of China. China's National Defense. 1998. http://www.china.org.cn/e-white/5/index.htm (Letöltés ideje: 2015. 08. 12.)
31 IISS: Military Balance 1998. p. 165.
32 Uo. p. 168.
33 IISS: Military Balance 1999. p. 175.
34 Uo. p. 171.
35 IISS: Military Balance 2001. p. 161.
36 Uo.

második tüzérség felépítése a Kommunista Párt Központi Bizottságának és a Központi Katonai Bizottság egyik fő stratégiai döntése …"

Hu Jintao elnök politikai kommunikációjába is beemelte a haderő technológiai fejlesztésének kérdését, főként a ballisztikusrakéta elleni védelmi képességek kiépítését és a „Második Tüzérség" fejlesztését. 2006-ban került hadrendbe a DF-31 ICBM, illetve megindult e típus további fejlesztése, mely az ambíciózus, 14.000 km-es hatótávolság elérését tűzte ki célul.

2007-2008 több szempontból is jelentős fordulópont Kína számára kül- és védelempolitikai szempontból egyaránt. Az olimpiák megrendezése jellemzően komoly globális szerepvállalási presztízskérdés Kelet-Ázsiában; Japán gazdasági sikereinek kezdetén, a világkereskedelembe való újbóli csatlakozásakor tartotta a '68-as ötkarikás játékokat, Dél-Korea pedig 1988-as házigazdagént az ország demokratizációs folyamatának nemzetközi elismerésével kötötte össze az eseményt. Kína 2008-as házigazda pozíciója leginkább egy egyre aktívabb globális szerepkörrel társult. A haderőfejlesztés szempontjából a legmarkánsabb előrelépések között kell említenünk a műholdak elleni támadó képességek terén elért fejlődést. A KNFH 2007-ben semmisített meg sikeresen egy kínai meteorológiai műholdat egy kétfázisú, szilárd hajtóanyagú rakétával, amelyet egy önjáró indítóplatformról lőttek fel.[37]

A 2010-es évekhez közelítve egyre látványosabbá vált a KNFH hozzáférést-gátló/területmegtagadó műveleti koncepcióhoz (anti-access/area denial – A2/AD) kötődő fegyverrendszereinek fejlődése. Az A2/AD célja olyan károkozási képességek kiépítése, amely a Kína közeli tengeri területeken csak jelentős kockázatok mellett teszi lehetővé egy ellenséges hatalom haditengerészetének mozgását. Ennek főbb elemei:

1) a hajó elleni ballisztikus rakéták (anti-ship ballistic missile – ASBM), ennek legfontosabb típusa a DF-21 MRB „D" változata, illetve hajó elleni cirkálórakéták fejlesztése (felszíni hajóegység-, tengeralattjáró- és repülőgép indítású változatoké egyaránt);
2) az ellenséges C4ISR rendszerek támadása, illetve zavarása, különös tekintettel a GPS működéséhez szükséges műholdak támadására;
3) fokozott partmenti védelem, tengeri akna, illetve hajó-elleni rakétával felszerelt partmenti hajóegységekre építve (ennek egyik ikonikus eleme a 2004-ben hadrendbe álllított Type 22 *Houbei* trimarán).

Az A2/AD képességek visszhangjaként az amerikai haderőfejlesztés – felismerve, hogy hogy Kína esetében ez alig leplezett módon főként az amerikai repülőgép-hordozó harccsoportok ellen irányult – az USA válaszul a fejlesztéseinek fókuszába az AirSea Battle műveleti koncepcióját helyezte és az elmúlt években egymással csak szoros összefüggésben értelmezhető fegyverkezési verseny alakult ki a KNK és az USA között.[38]

---

[37] IISS: Military Balance 2008. p. 359.

[38] Az A2/AD és az AirSea Battle koncepciójáról részletesebben lásd.: KISS Roland: Air-Sea Battle – A globális közös terekhez való hozzáférés hadműveleti koncepciója. Nemzet és Biztonság 2015/4. pp. 56-69.

Kína 2009-2010-re már vélhetően 1000 ballisztikus rakétát vonultatott fel Tajvan szigetével szemben, ám a sziget és a KNK viszonya viszonylagos enyhülési pályára került Ma Ying-jeou, a Kuomintang (KMT) pártvezetőjének megválasztásával. Ellentétben elődje, Chen Shui-bian „szeparatista" politikájával, Ma sokkal konszolidáltabb partnernek bizonyult a szoros-közi viszonyok kapcsán. Érdekes külpolitikai váltás volt azonban az orosz részről egyre hangosabbá váló kritika, miután Oroszország egyre jobban kezdte sérelmezni a KNFH orosz eredetű fegyverrendszereinek „*reverse engineering*" tevékenységét, vagyis a megvásáról orosz haditechnológia engedély nélküli és látványos lemásolását. Ennek a problémának emblematikus eleme a Shengyang J-11B vadászgéptípus, mely javarészt a Szu-27 „koppintásaként" jött létre.[39]

Egyre inkább úgy tűnik, hogy korszakváltásnak is tekinthető a pártfőtitkári hatalomátadás időszaka 2012-ben, mely során Hu Jintao-t Xi Jinping váltotta a KNK vezetői pozíciójában. Ez év a KNFH szempontjából szintén komoly fordulópontot jelentett, méghozzá kifejezetten az erőkivetítési képességek fejlesztése terén. Ekkor helyezték üzembe ugyanis az első kínai repülőgép-hordozót.

2015-ben, a második világháború győztes befejezésének évfordulójához kötődően Xi Jinping további átfogó reformokat hirdetett a védelmpolitika terén. Egyrészt 300.000 fővel kívánta csökkenteni a haderő létszámát. Másrészt átfogó szervezeti átalakításokat is megkezdtek. A korábbi hét katonai körzet rendszerét felváltotta az öt összhaderőnemi hadszíntéri főparancsnokság.

A 2015-ben kiadott, legutóbbi védelmi fehér könyv a korábbiakhoz képest jóval nagyobb hangsúlyt fektet a tengeri hadviselés fontosságára. A haderőfejlesztés és modernizáció, a haditengerészeti komponens kiemelése és ehhez társulva Kína egyre nagyobb külpolitikai aktivitása azonban nem jelenti azt, hogy a KKP szakítana alapvetően defenzív retorikába ágyazott védelmi doktrínájával. A 2015-ös fehér könyv egyik fejezetének címe „*III. Az Aktív Védekezés Stratégiai Irányelvei*", szemléltetve, hogy a kínai vezetés szükségesnek érzi egyre látványosabb katonai képességeit védekező alapvetésekre épülő narratívába helyezni.[40]

A Xi Jinpinghez köthető korszakváltásra már egyértelművé válik az a folyamat, ami a haderőnemek közötti arányok átalakulását jellemezte 1989 óta. Az elmúlt években – úgy tűnik – a KNFH Szárazföldi Haderőneme sokat veszített korábbi politikai prioritásából. Az új fegyverrendszerek és fejlesztési projektek alapján úgy látszik, a többi haderőnem jóval nagyobb mértékben esik át korszerűsítésen.[41]

A 2015-ben elindult reformfolyamatok részeként a korábban „Második tüzérségként" ismert hadászati rakétacsapatok fegyverneme önálló haderőnemi szintre emelkedett, Hadászati Rakétaerőkként. A következő években várhatóan hadrendbe áll a legújabb ICBM típus, a DF-41-es, bár erről még pontosabb információ egyelőre nincs, de a Hadászati Rakétaerők szervezeti felépítése alapján

---

[39] IISS: Military Balance 2010. pp. 376-377.

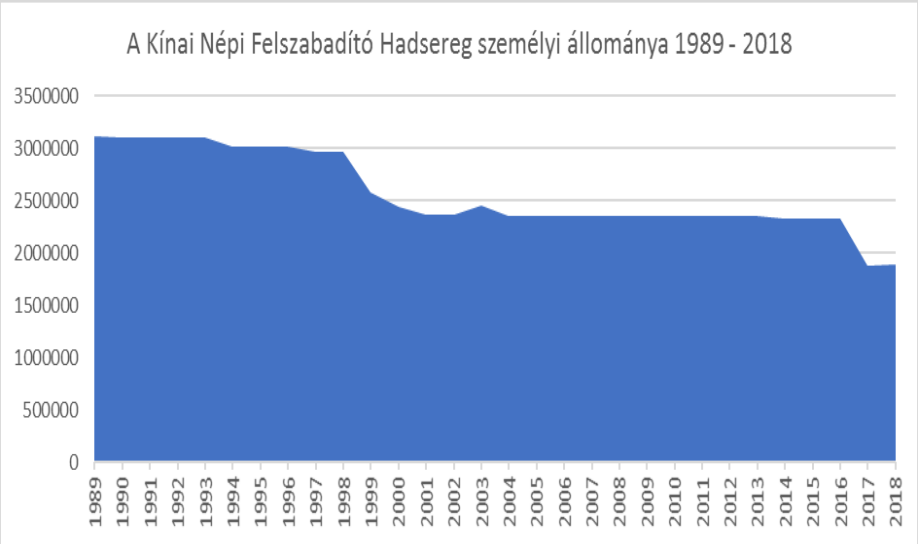
[40] The State Council Information Office of the People's Republic of China. China's Military Strategy. 2015 http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm (Letöltés ideje:2018. 08. 12.)

[41] IISS: Military Balance 2016. p. 222.

már többen feltételezik, hogy bizonyos egységek eleve az új típus várható bevezetése kapcsán jöttek létre.[42]

Bár a tengeri erőkivetítési képesség egyes elemei továbbra is hiányoznak, Kína első külföldi bázisának megnyitásával – Djibouti-ban – már elindult egy jóval nagyobb globális mozgástér kiépítésének irányába.[43]

Peking 30 év leforgása alatt széles körű és eredményes modernizációt volt képes végrehajtani a fegyveres erőkön belül. Ezzel együtt járt egyrészt a személyi állomány fokozatos csökkentése, valamint a védelempolitika fókuszának fokozatos áttevődése a szárazföldi haderőnem központú, területvédelmi berendezkedéstől az „aktív védelem" koncepciójának megfelelően az elrettentés és erőkivetítés eszköztárával rendelkező haderő irányába. Az 1989-ben több mint 3 millió fős kínai haderő, mely már feltehetően ekkorra átesett korábbi állományi „karcsúsításon", 2,3 millió fős szárazföldi komponense jól mutatja a szemléleti váltást a mai állapotokhoz képest. A KNFH teljes létszáma 2018-ban kicsivel több mint 1,8 millió fő, ám az öt haderőnem közül a szárazföldi komponens ma alig több, mint a létszám felét teszi ki 975.000 fővel.



4. ábra

A KNFH állományi létszáma 1989-2018 között:

1989	**1990**	**1991**	**1992**	**1993**	**1994**
3.120.000	3.100.000	3.100.000	3.100.000	3.100.000	3.020.000

1995	**1996**	**1997**	**1998**	**1999**	**2000**
3.020.000	3.020.000	2.965.000	2.965.000	2.580.000	2.440.000

[42] Uo. p. 228.
[43] Uo. p. 227.

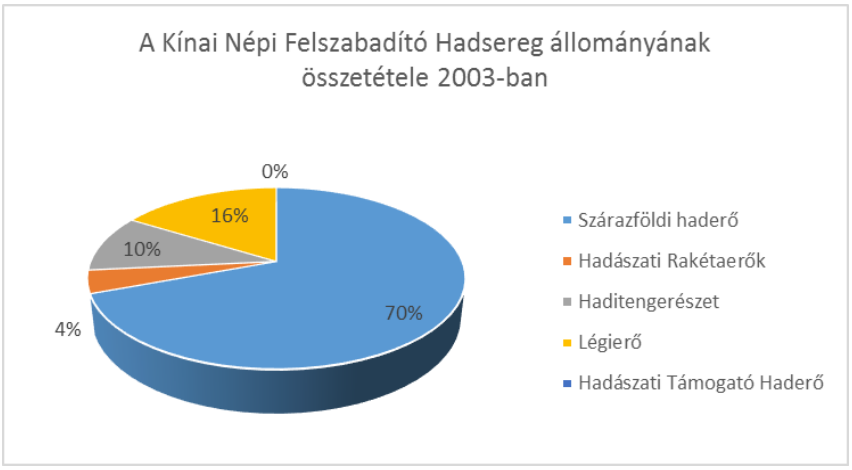
2001	2002	2003	2004	2005	2006
2.370.000	2.370.000	2.450.000	2.355.000	2.355.000	2.355.000

2007	2008	2009	2010	2011	2012
2.355.000	2.355.000	2.355.000	2.355.000	2.355.000	2.355.000

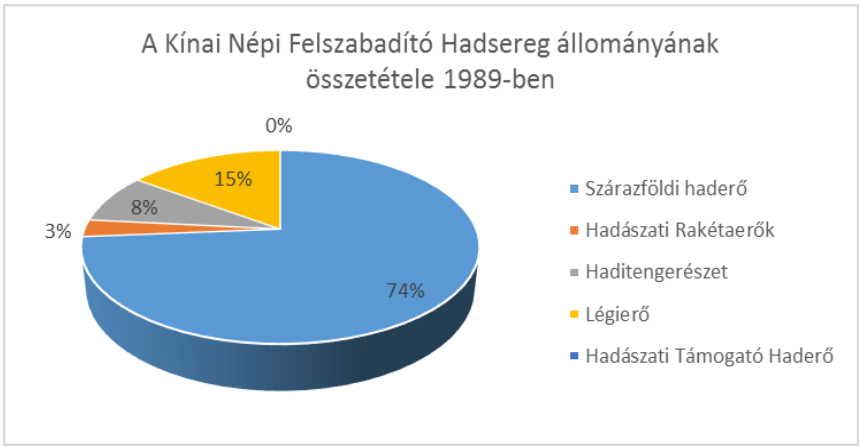
2013	2014	2015	2016	2017	2018
2.355.000	2.333.000	2.333.000	2.333.000	1.883.000	18.85000

5. ábra

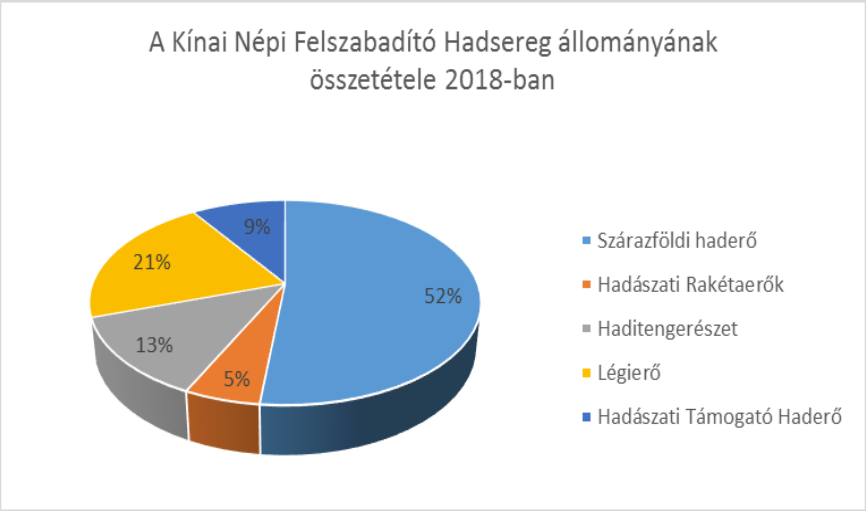
A haderőnemek közötti eloszlás alakulása 15 évenkénti bontásban jól mutatja a fokozatos átalakulást a KNFH szervezetében.



6. ábra



7. ábra



8. ábra

A KNFH átalakulásán megmutatkozik Kína geopolitikai szerepvállalásának és ambícióinak átalakulása is. A hidegháború végén, a kínai-szovjet enyhülés kezdeti szakaszában a szárazföldi védelem kérdése érthető módon uralta a kínai stratégiai gondolkodást.

Mára azonban Kína, mint a második legnagyobb globális gazdasági hatalom amely egyre aktívabb külpolitikát folytat, már nem kötődhet Deng Xiaoping „türelemmel váró" elképzeléseihez. A tenger irányába történő nyitás egyszerre mutat új lehetőségeket és ad új fenyegetés-percepciót Kína számára. A KNK geopolitikai helyzetének tengeri irányú szemléletében kulcsfontosságot játszik a Kínát bekerítő „első- és második szigetláncok" koncepciója. Ennek lényege, hogy a második szigetlánc (Alaszka, Kamcsatka félsziget, Japán, USA csendes-óceáni szigetei) és az első szigetlánc (Japán teljes hossza, Tajvan, illetve a Dél-Kínai-tenger körül elhelyezkedő délkelet-ázsiai országok) szükség esetén képesek bezárni Kína kijutását a világtengerekre. Úgy tűnik, hogy az átalakulás következő lépéseként a KNFH számára a jövőben ezen kihívás megoldása lesz az elsődleges cél, persze továbbra is az „aktív védelem" jegyében. A haderőfejlesztés általános történeti áttekintése után érdemes azonban kitérnünk a haderőnemek átalakulására is az elmúlt három évtizedben.

Kínai Népi Felszabadító Hadsereg – Szárazföldi Haderőnem

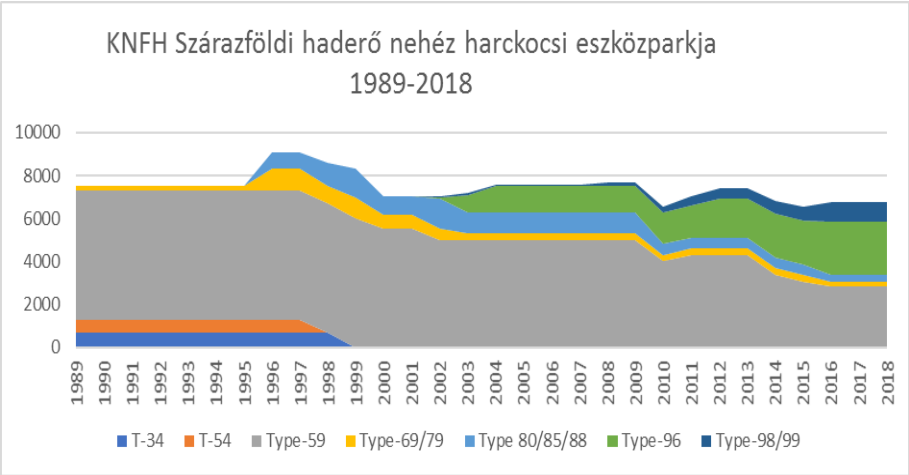
A KNFH Szárazföldi Haderőneme sokáig a kínai fegyveres erők egyértelműen központi politikai prioritást élvező eleme volt, különösképpen a Tiananmen téri tüntetések leverésében vállalt szerepét követően. Mára azonban úgy tűnik, sokat veszített privilegizált helyzetéből, bár valószínűleg még mindig a legnagyobb politikai befolyással rendelkező haderőnem.

A szárazföldi erők diszlokációja 1989-től 2016-ig hét katonai körzetre oszlott. A szárazföldi erők csapatai 24 „*hadseregcsoportra*" (集团军 *csoport-hadsereg,* angol fordításban *group army*) oszlott, amelyet az angol szakirodalom általában a

hadtesttel egyenértékű magasegységként kezel. A „hadseregcsoportok” állományában összesen 80 lövész hadosztály, 10 páncélos hadosztály és 6 tüzér hadosztály állt. 1989-ben ezt még kiegészítette egy 3 hadosztályból álló légideszant hadtest és 1 önálló hadosztály.

A 2015-16-os átszervezéseknek köszönhetően a Hadszíntéri Parancsnokságok létrehozása mellett a szárazföldi haderőnem szervezeti felépítése is megváltozott. A korábbi 24 helyett mára 13 „hadseregcsoport” maradt, alárendeltségükben 15 különleges műveleti, 23 harckocsi dandár, 1 harckocsi hadosztály, 1 gépesített lövész hadosztály, 23 gépesített lövész dandár, 3 könnyű lövész hadosztály, 27 könnyű lövész dandár, 2 ejtőernyős dandár, 6 partraszálló dandár, és további logisztikai és támogató egységek állnak.

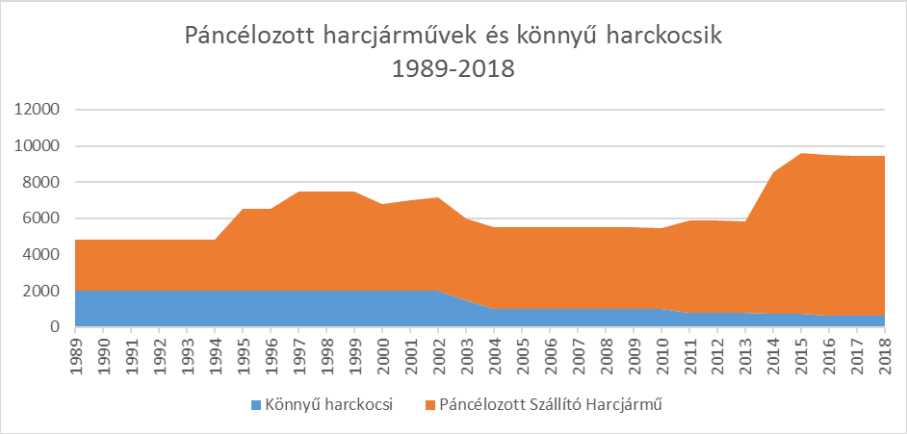
Eszközparkjának főbb elemeit 7500 harckocsi és 1200 könnyű harckocsi adta, illetve 2800 szállító- és gyalogsági harcjármű. A tüzérségi eszközök összetételéről a ’90-es évek elejét tekintve nincsenek pontos számok, de nagyjából 14500 vontatott löveg (100mm; 122mm; 130mm; 152mm), önjáró lövegek (amelyek 1989 darabszáma 2003-ig nem ismert, akkor 1200 darab) és 3800 rakéta sorozatvető. A nehézeszközök javarészt szovjet eredetű, esetleg annak hazai fejlesztésű változatai.



9. ábra

Az eszközpark változásának két főbb iránya 1989 óta egyrészt a harckocsi eszközpark korszerűsítése, illetve a páncélozott szállító- és gyalogsági harcjárművek állományának fokozatos bővítése. Előbbi téren az 1989-ben még a javarészt hatvanas évek szintjét képviselő Type-59-es nehézharckocsi (a szovjet T-54-es kínai változata) kivezetésével fokozatosan nőtt a korszerűbb, hazai fejlesztésű típusok aránya. Mára a harckocsi eszközpark derékhadát a Type-59 mellett a Type-96 vagy ZTZ-96 adja, mely a kilencvenes évek végén állt hadrendbe és mára 2500 áll rendelkezésre.

A harckocsi eszközpark átalakulása mellett a szállító- és gyalogsági harcjárművek száma szintén komoly növekedésen ment keresztül, mára majdnem kétszer annyi eszköz áll rendelkezésre, mint 1989-ben (1989: 4500 db; 2018: 8820).



10. ábra

A szállító- és gyalogsági harcjárművek összetételéről nem minden év esetében áll rendelkezésre adat, de a 2000-es évektől kezdve lényegében látszik a szovjet eredetű eszközök kivonása és azok fokozatos váltása „hazai" fejlesztésű haditechnikával:

	2002	**2010**	**2014**	**2018**
BMD-3	100	0	0	0
Type-03 ZBD ZBD-03	0	40	0	0
Type-04 ZBD-04	0	300	750	900
Type-05 AAAV ZBD-05	0	200	300	300
Type-08 ZBL-08	0	0	0	720
Type-09 ZBL-09	0	100	400	0
Type-523	60	0	0	0
Type-551	600	0	0	0
Type-63	3000	2000	1650	2400
Type-77 (BTR-50PK)	200	200	0	0
Type-85/89 (YW-531H)	400	300	1500	1750
Type-86	800	600	1250	1250
Type-92	0	600	1850	1200
WZ-523	0	100	100	0

11. ábra

A szárazföldi erők alakulása a KNFH elmúlt három évtizedében főként az állomány optimalizációjára, illetve a mozgékonyság növelésére fókuszált, ahogy az látszik a hadsereg létszámának csökkenésén és a szállítójárművek eszközparkjának növekedésén.

Kínai Népi Felszabadító Hadsereg – Haditengerészet

A KNFH haditengerészete fokozatosan nyerte el mai, kiemelt helyzetét Kína globális szerepvállalásának változása, valamint a haderőnem fejlesztéseinek köszönhető jelentősebb képességnövekedéseknek köszönhetően. A haditengerészeti képességek fejlődésének üteme többeket meglepetésként ért az ezredfordulón. Mindezt mutatja, hogy alig tíz év alatt hogyan változott meg az USA globális érdekeire vonatkozó fenyegetettség percepciója Kína kapcsán. 1996-ban még bevett kiszólásnak számított, hogy Kína egyetlen opciója Tajvan elfoglalására egy „egymillió emberes úszás" lehetne,[44] alig egy évtizeden belül már komoly témává vált Kína tengeri haderejének fenyegető növekedése.

A kilencvenes évekhez közeledve a haditengerészet számára elsősorban az elavult felszíni egységek kivezetése és a tengeralattjárók fejelsztése volt előirányozva. A *Han* tengeralattjáró osztályt a fejlettebb *Xia* volt hivatott váltani, ám technológiai hibáknak köszönhetően a tervezett két egység helyett csak egy tudott hadrendbe állni.[45]

A felszíni egységek korszerűsítése azonban sikeresebbnek bizonyult, a KNK felújította két *Luda* típusú rombolóját és további, helikopterrel felszerelt hajókat tudott hadrendbe állítani 1990-ben.[46]

1993-ban a tengeralattjárófejlesztés korábbi kudarcaival ellentétben sikerült jelentősebb előrelépéseket tenni, a haditengerészet hadrendbe állított 6 – kifogásolható állapotuk miatt korábban leszerelt, de később felújított – *Ming* osztályú tengeralattjárót. '93-ban továbbá már a nemzetközi közvélemény számára is kiderült, hogy a KNK repülőgép-hordozó beszerzését, vagy fejlesztését tervezi.[47]

Az első, teljesen kínai fejlesztésű tengeralattjáró, a dízelmeghajtású *Song* osztály prototípusa 1998-ban került tesztüzembe, ami már a kínai védelmi ipar önállósodásának fontos mérföldköveként is értékelhető.

A flottafejlesztés részeként Kína két *Szovremennij* osztályú rombolót rendelt az ezredfordulón, illetve két hazai fejlesztésű *Luhai* osztályú romboló beszerzését és hadrendbe állítását ütemezte elő.[48] Ezen felül nyolc orosz *Kilo* osztályú dízel-elektronikus meghajtású tengeralattjáró beszerzéséről döntöttek.[49]

Kína haditengerészete a 2000-es évek elején kezdte el „9935-es projektet", vagyis a KNFH Ukrajnából bontásra vásárolt repülőgép-hordozójának átalakítását.[50]

---

44 TYLER, Patrick: China's Military Stumbles even as Its Power Grows. New York Times 1996. Dec. 3. https://www.nytimes.com/1996/12/03/world/china-s-military-stumbles-even-as-its-power-grows.html (Letöltés ideje: 2018. 08. 12.)

45 Uo.

46 IISS: Military Balance 1991. p. 149.

47 IISS: Military Balance 1993. p. 163.

48 IISS: Military Balance 2002. p. 139.

49 Uo.

50 IISS: Military Balance 2004. pp. 259-314.

Az átalakítások után a KNFH első repülőgép-hordozóját, a *Liaoning-et*, 2010 szeptemberében bocsátották vízre.[51] Nagyjából ekkor, a KNFH Haditengerészetének kötelékén belül működő tengerészgyalogság is szervezeti reformokon esett át. A feltehetően optimalizációt célzó szervezeti átalakítások után a felszereléseken is fejlesztettek. A tengerészgyalogos dandár a legújabb típusú, a kínai Norinco vállalat által gyártott Type 05-ös kétéltű harci járművekel (ZBD-05 kétéltű gyalogsági harcjármű és ZTD-05 kétéltű könnyű-harkocsik), míg a 164. tengerészgyalogos dandár kapta meg a régebbi típusú Type-63 páncélozott szállítójárművek kétéltű változatait.[52]

A 2010-es vízrebocsájtást követően a *Liaoning* két évvel később, Shenyang J-15 vadászgépek (a Szu-33-as, repülőgép-hordozóra kialakított változata) és Z-8-as helikopterekkel felszerelve kezdte meg próbaüzemét.[53] A hajóegység valószínűleg inkább kiképzési célokat szolgál, illetve a későbbi, hazai gyártású repülőgép-hordozók mintájául szolgál. A repülőgép-hordozók hadrendbe állítása mellett azonban egyelőre a KNFH számára az erőkivetítési képességeket jelentősen korlátozza a logisztikai hajóegységek és külföldi bázisok korlátozott száma.

A haditengerészet 2015-re már két új, korszerűségét tekintve már a világ többi tengeri hatalmával összemérhető rombolót állított hadrendbe a Type-052D *Luhu*-osztályból. A korábbi típusokhoz képest ebből valószínűleg nagyobb mennyiségű készül majd, vélhetően ezek fogják majd váltani az elkövetkező években kiöregedő rombolókat.[54] A felszíni hajóegységek bővítésének további lépése a Type-055 *Renhai* cirkáló osztály,[55] amelyből az első egység feltételezhetően 2018-ban áll hadrendbe, illetve Kína második repülőgép-hordozója, vélhetően 2020-ig.[56]

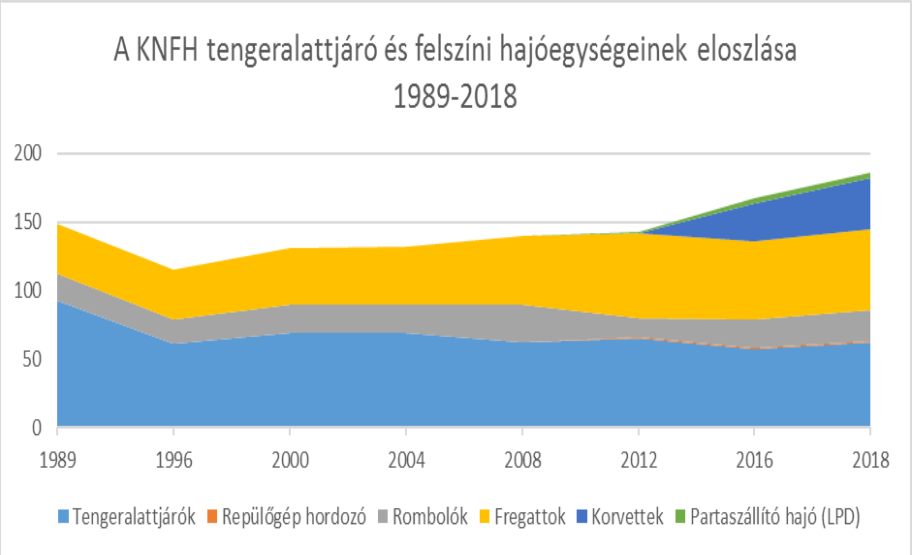
Míg a 2015-16-os védelempolitikai reformok jelentősebb strukturális változásokkal jártak a szárazföldi haderőnél, a haditengerészet diszlokáció nem sokat változott az elmúlt évtizedekben. Egységei három flottára oszlanak, az Északi-tengeri-fotta (**北海**舰队, North Sea Fleet), központi kikötője Qingdao, a Keleti-tengeri-flotta (东海舰队, East Sea Fleet) központja Ningbo és a Déli-tengeri-flotta (**南海**舰队 South Sea Fleet) központja Zhanjiang.

51 IISS Military Balance 2011 p. 191.
52 IISS Military Balance 2011 p. 196.
53 IISS Military Balance 2013. p. 252.
54 Uo. p. 224.
55 IISS Military Balance 2016. p. 224.
56 IISS Military Balance 2018. p. 232.

	Hajótípusok	1989	2000	2012	2016	2018
Repülőgép hordozó	Liaoning (Type 001)	0	0	1	1	1
Cirkáló	Renhai (Type 055)	0	0	0	0	1
Romboló	Hangzhou (Szovremennij)	0	0	4	4	4
	Luyang I (Type-052B)	0	0	2	2	2
	Luyang II (Type-052C)	0	0	3	6	6
	Luyang III (Type-052C)	0	0	0	4	6
	Luhai (Type-051B)	0	0	1	1	1
	Luhu (Type-052)	0	2	2	2	2
	Luzhou (Type-051C)	0	0	2	2	2
	Luda	17	16	0	0	0
	Anshan (Gordy)	2	0	0	0	0
Fregatt	Jiangkai I (Type-054)	0	0	2	2	2
	Jiangkai II (Type-054A)	0	0	13	22	25
	Jiangwei I (Type 053H3)	0	4	4	0	0
	Jiangwei II (Type-053H2G)	0	0	10	10	10
	Jianghu (Type 053)	26	30	23	19	16
	Luda (Type-051)	0	0	10	4	4
	Jiangdong (Type 053)	2	0	0	0	0
	Jiangnan (Type 053)	5	0	0	0	0
	Chengdu (Type 053)	4	2	0	0	0
Korvett	Jiangdao (Type-056)	0	0	0	27	37

11. ábra: A haditengerészet hajótípusai

A kínai flotta felszíni egységeinek kékvízi képességek irányába történő elmozdulása jelenleg is zajló folyamat, amely javarészt a 2010-es években kezdődött. Várhatóan a jövőben ezen lesz a fő hangsúly, valamint a partaszállító képességek növelésén. Ez utóbbi legfontosabb elemét képezi a jelenleg használatban levő 4 Yuzhao osztályú (Type-071) partaszállító hajó, melyek szállítókapacitása 4 légpárnás partraszállító naszád, 4 helikopter, 60 páncélozott harcjármű és 800 fő. Kína tengerészgyalogsága a haditengerészet köteléke alá tartozik, ezen belül is a déltengeri flotta fennhatósága alá. Létszáma 1989-ben 6000 fő volt, ez a ’90-es években 10.000 főre nőtt, ma 15.000 fős.

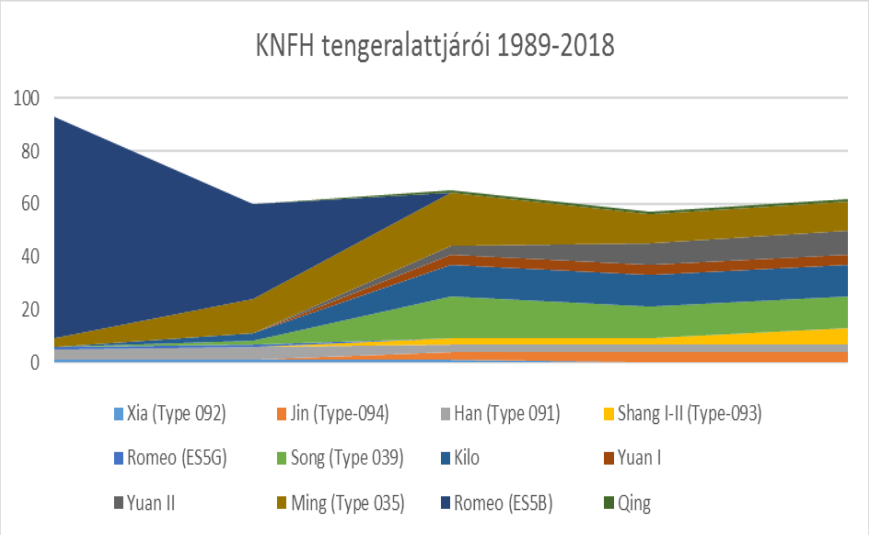


12. ábra

A felszíni hajóegységek és a tengerészgyalogság fejlődése mellett érdemes kitérni a tengeralattjárók fejlesztéseinek folyamataira. A KNFH tengeralattjáró flottájának átalakulása szoros összefüggésben állt Kína A2/AD képességeinek kiépítéséhez, illetve a tajvani krízis utáni, stratégiai elrettentésre fókuszáló haderőfejlesztési folyamatokkal. Fokozatosan került kivonásra a szovjetektől a hatvanas években beszerzett *Romeo* osztály, amelyekből 1989-ben rendelkezésre állt 85 egység. A 2010 utáni évekre a megmaradt darab már csak kiképzési célt szolgál. Kína a nyolcvanas években önállóan fejlesztett *Xia* osztályú atomtengeralattjárója sikertelen projektnek bizonyult. Az ezredforduló után gyártani kezdett *Jin* osztály azonban már nagyobb sikerrel járt, jelenleg 4 eszköz készült el és további 4 várható a jövőben. Szintén atommeghajtású osztályok a *Han* és a *Shang I* és *II* változatok. A tengeralattjáró flotta javát azonban a dízel-elektromos változatú eszközök adják. Ezen belül 1989 óta a lényegi változás a *Romeo* osztály eltűnése és helyette a hazai fejlesztésű típusok elterjedése.

	Típusok	1989	2000	2012	2016	2018
Atom-meghajtású	Xia (Type 092)	1	1	1	0	0
	Jin (Type-094)	0	0	3	4	4
	Han (Type 091)	4	5	3	3	3
	Shang I-II (Type-093)	0	0	2	2	6
Dízel-elektromos	Romeo (ES5G)	1	1	0	0	0
	Song (Type 039)	0	1	16	12	12
	Kilo	0	3	12	12	12
	Yuan I	0	0	4	4	4
	Yuan II	0	0	3	8	9
	Ming (Type 035)	3	13	20	11	11
	Romeo (ES5B)	84	36	0	0	0
	Qing	0	0	1	1	1

13. ábra: Tengeralattjáró flotta típusai



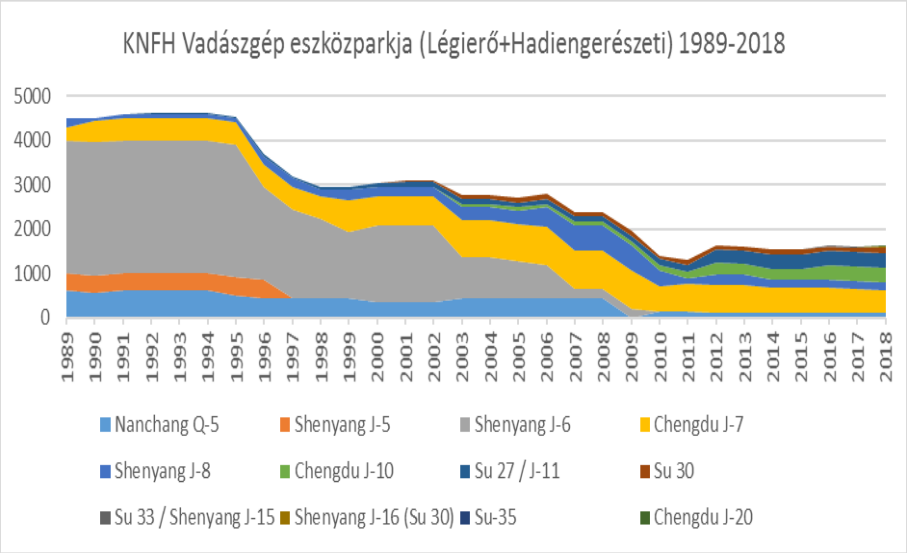
14. ábra

Kínai Népi Felszabadító Hadsereg – Légierő

Kína légiereje – a haditengerészethez hasonlóan – harminc éve főleg területvédelemre volt alkalmas, mára viszont egy egyre nagyobb akciórádiuszú és modernebb haderőnem benyomását kelti.

A korszerűsítés folyamata ténylegesen a ’90-es évek végén indult el, a Szu-27-es vadászgépek beszerzésével, majd ezt követően a hazai fejlesztésű negyedik

generációs vadászgépek gyártásának megkezdésével.[57] Ezek nagy része jelentősen épített a korábban vagy a későbbiekben beszerzett orosz modellekre, kivételt képez a már említett Chengdu J-10-es, mely valószínűleg több hazai és külföldi típus sajátosságaira is épít, ám fejlesztése körül külön port kavart, hogy valószínűleg izraeli eredetű technológia képezte az alapját, ami feszültségeket okozott az USA és közel-keleti szövetségese között.[58]

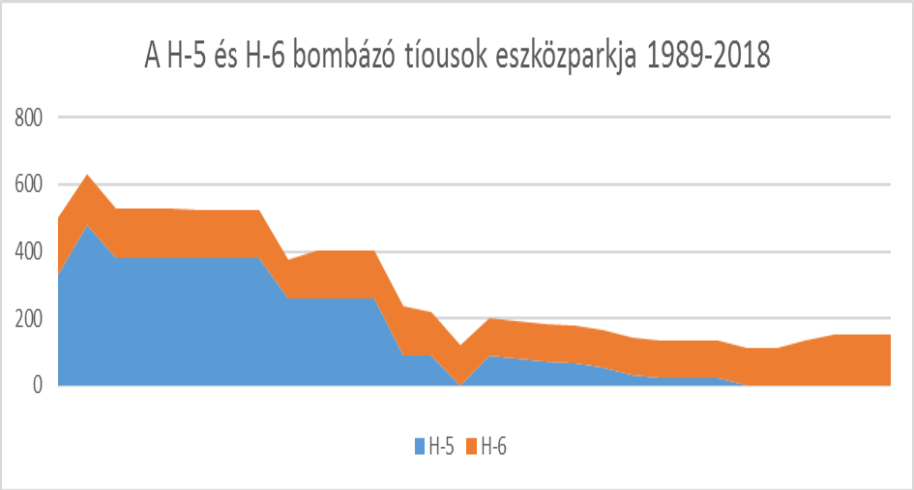


15. ábra

A vadászgép eszközpark 1989-től tartó átalakulásának köszönhetően – a nagymértékű leépítés mellett – a kilencvenes évek javarészt szovjet géptípusainak aránya mára jelentősen lecsökkent és a korszerűbb, újabb generációs géptípusok jóval nagyobb arányban képviseltetik magukat.

A bombázók terén az elmúlt harminc évben két géptípus volt használatban, így a Xian H-6 (a Tu-16-os kínai változata), melynek darabszáma kevés változások mellett ma 150, ami kis csökkenés az 1989-es 170-hez képest. A másik típus a H-5 (az Il-28 kínai változata) amelyből 1989-ben 330 állt hadrendben, ám az ezredfordulótól kezdve fokozatosan kivonták a szolgálatból.

[57] Uo. p. 146.
[58] ADELMAN, Jonathan: The Phalcon Sale to China: The Lessons for Israel. Jerusalem Center for Public Affairs, 2002. p. 474.



16. ábra

A légierő fejlesztéseinek későbbi szakaszát jelentette a korai előrejelzés és megfigyelési képességeinek javítása 2006-tól, aminek keretében Kína megkezdte egy hazai gyártású géptípus, az Il-76-os modelljére épülő Kong Jing 2000 (KJ-2000) fejlesztését.

Kínai Népi Felszabadító Hadsereg – Hadászati Rakétaerők

A mai nevén Hadászati Rakétaerőkként önálló haderőnemmé alakított, korábban „második tüzérségként" ismert haderőnem kezeli a KNFH ballisztikusrakétáit és a hozzájuk tartozó nukleáris robbanófejeket.
Eszközeinek jelentős többségét rövid- és közepes hatótávolságú rakéták adják, Oroszországhoz vagy az Egyesült Államokhoz képest Kína relatíve kevesebb ICBM-el, illetve atomtöltettel rendelkezik. Nukleáris doktrínája a válaszcsapásra épülő elrettentésre alapoz.

Felismerve a technológiai lemaradás jelentette veszélyeket, 1992-ben Kína új ballisztikusrakéta típusok fejlesztésébe kezdett, lecserélendő a korszerűtlenné vált ICBM típusokat, rakéta eszközparkja kapcsán azonban további nemzetközi kritika vetült a KNK-ra, amiért feltételezhetően korábbi típusai közül adott el Iránnak és Szíriának.[59]

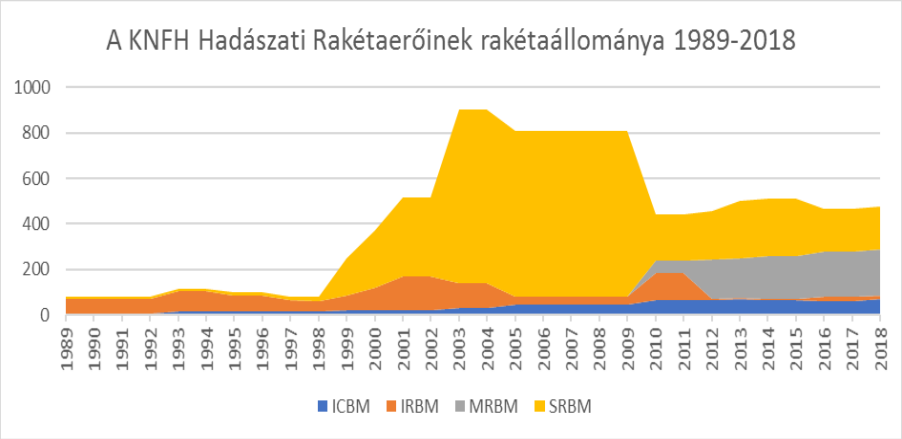
1994-ben két új ballisztikusrakéta fejlesztésre is fény derült. Az egyik egy kettős felhasználású típus, a szárazföldi indítású változat a DF-31 (8000 km hatótávolsággal), illetve ennek tengeralattjáró indítású változata a JL-2. A második, a DF-41-es az eddigi legnagyobb hatótávolságú, szárazföldi indítású típus, várhatóan 12 000 km-es hatósugárral, ám ez még máig nem állt hadrendbe.[60]
A kilencvenes években nagyobb előrelépést jelentett a KNFH „Második Tüzérségre" épülő, Tajvannal szembeni elrettentési képességeinek fejlesztése. A

[59] IISS: Military Balance 1992. p. 139.
[60] IISS: Military Balance 1994. p. 164.

KNK folyamatosan növelte a szigethez közeli területein állomásoztatott rakétáinak számát.

A KNK három fontosabb új stratégiai ballisztikus rakétát fejlesztését folytatta a ’90-es években, a 8000 km hatósugarú DF-31-es ICBM-et; a 12000 km hatósugarú DF-41-es ICBM-et; illetve a tengeralattjáró indítású JL-2 SLBM-et.

A Hadászati Rakétaerők legnagyobb fejlesztési hulláma a szárazföldi Kína és Tajvan közötti 1995-96-ban kialakult – a korábbinál – feszültebb viszony után lendült meg látványosan, az óta kisebb nagyobb változások voltak ugyan, de a közeljövő igazán jelentős minőségi változása a DF-41-es ICBM hadrendbe állítása lesz majd. Jelen tanulmány készültekor ugyan feltételezhető, hogy a DF-41-es a közeljövőben hadrendbe áll – egyes értesülések szerint a kezelőszemélyzetnek már megvan a szervezeti helye a „Második Tüzérség” kötelékén belül, de jelenleg még feltételezhetően a rakétaeszközök nincsenek hozzárendelve a kötelékhez.



17. ábra

Szintén egy új önálló fegyvernem szervezeti szintjeként jött létre 2016-ban a korábban a logisztikai feladatokat, információs hadviselést és kibervédelmet, valamint a katonai űrporogramot végző szervezeti egységek összevonásából, a Hadászati Támogató Haderő. Ennek feladatköre az információs és kibervédelem, az űrvédelem, a kutatás és fejlesztés, valamint a logisztikai támogató tevékenység koordinálása. A reformok eredményeiről várhatóan 2020-ra lesz pontosabb képünk, de az eddigi fejlemények alapján a KNFH jó úton halad a kijelölt célok teljesítése felé.[61]

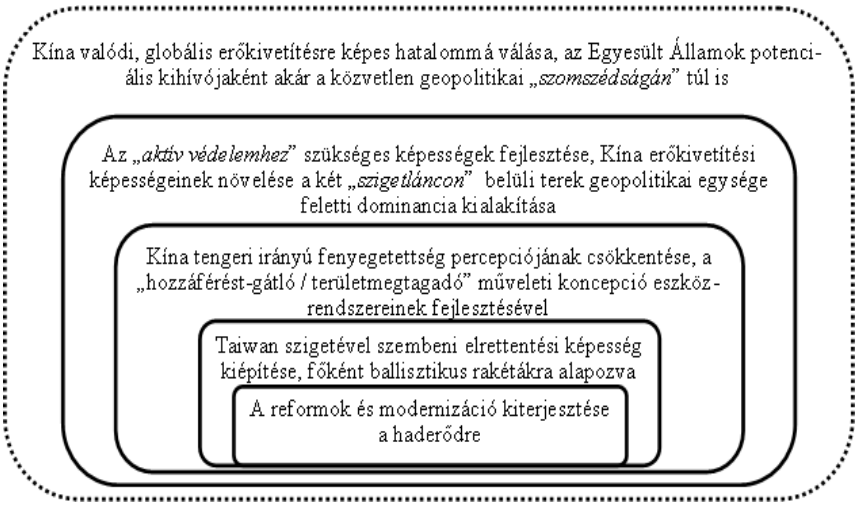
Összegzés – Kína harminc éves útja a katonai modernizáció terén

A Kínai Népköztársaság komoly kihívásokkal állt szemben a bipoláris világrend felbomlásakor, még ha ezek sok esetben első ránézésre nem is voltak szembetűnőek a Deng Xiaoping korszakában bámulatos gazdasági fejlődési pályán

[61] IISS: Military Balance 2018. pp. 225-226.

elinduló ország vezetése vagy a nemzetközi közösség számára. Kína egyrészt kedvezőtlen geopolitikai elhelyezkedésének köszönhetően komoly bezártság percepcióval szemléli a globális terekhez való viszonyát, másrészt 1989-ben – a kínai katonai modernizáció még igencsak gyerekcipőben járó időszakában – a Tiananmen téri események miatt, a korábbiakhoz képest elszigetelt nemzetközi pozícióban találta magát.

A szovjet, majd orosz eszközök beszerzése némileg enyhítette a nyugati fejlett technológiákhoz való hozzáférés nehézségét, ám a kínai védelmi ipar igazán csak az ezredforduló utáni időszakban tudta felvenni a rég várt modernizáció kellő ritmusát.



18. ábra: Védelempolitikai reformok

A védelempolitikai reformok és a haderő fejlesztésének történetét szemlélve Kína ezidáig négy fontosabb hullámmban tudott változtatni pozícióján és ezen folyamatnak szerve folytatása lehet a ma látszódó fejlesztések alapján a globális mozgástér bővítése. 1989-től a '90-es évek közepéig Kína főleg a haderő létszámcsökkentésére és az kezdeti szintű korszerűsítésre összpontosított. A tajvani krízist követően elsősorban a szigettel szembeni elrettentési képességek növelése volt a cél, főként a ballisztikusrakéták fejlesztésével és azok nagy számú felhalmozásával a sziget kapcsán stratégiai fontosságú régiókban. Miután Kína magabiztosabbnak érezhette magát Tajvannal szemben, a következő lépcső az első szigetláncon belüli „elrettentési" képesség, az A2/AD eszközrendszereinek fejlesztése lett, javítva Kína hatalmi pozícióját az Egyesült Államok és szövetségeseivel szemben. Miután a 2010-es évekre Kína jogosan érezhette, hogy az amerikai repülőgép-hordozó harccsoportok „büntetlen" mozgástere jelentősen szűkült, az A2/AD fókuszú fejlesztéseket felváltotta a tengeri „aktív védelem" koncepciója, vagyis a kékvizi flotta és a közvetlen régión belüli erőkivetítési képességek fejlesztése. Ezek után logikus folytatásnak tűnhet, hogy – miután a KNK magabiztosnak érzi majd „aktív védekezésen" alapuló képességeit, feltehetően a „második szigetlánc" vonaláig –, a jövőben Kína globális érdekeinek védelméhez szükséges, valóban globális erőkivetítési képességeket fejleszt.

Felvetődik a kérdés, hogy mindez elvezet-e majd konfrontációhoz az Egyesült Államokkal? Ez nagyban függ majd a Kína erősödésére adott globális válaszoktól, de vélhetően attól is, hogy a kínai vezetés mennyiben érzi hatalma legitimitásának szempontjából szükségesnek a konfrontáció felvállalását. Kína haderőfejlesztési ciklusai szoros összefüggésbe vonhatók a KKP és a kínai vezetés politikai mozgásterével. Tajvan szeparatista törekvéseinek kérdése alapjaiban rengetheti meg a KKP legitimitását, így feltehetően ez áll a geopolitikai érdekek középpontjában. Ezt követi Kína tágabb értelmű szuverenitásának védelme, amely biztosítását szolgálja az A2/AD képességek eszköztára. Ennél már a KKP politikai legitimitásának kérdésétől egy lépéssel távolibb, de továbbra is fontos szempont a Kína számára fontos tengeri útvonalak biztosítása, amit elősegít a tengeri „aktív védelem".

Az, hogy az egyre táguló kínai védelempolitikai látókör külső szelete mennyiben jelent majd konfrontatív álláspontot, nagyban függ majd attól, hogy a KNK Xi Jinping második ciklusában milyen narratívában kommunikálja majd Kína globális hatalommá válását és várhatóan a további haderőfejlesztések mértéke és azok kivitelezése is függ majd attól, mennyire érzi a pekingi vezetés mindezt nélkülözhetetlennek a jövőben.

Felhasznált források:

- ACHARYA, Amitav. Thinking theoretically about Asian IR. International relations of Asia, 2014, In: SHAMBAUGH, David – YAHUDA, Michael (ed.). International relations of Asia. Rowman & Littlefield, 2014.
- ADELMAN, Jonathan. The Phalcon Sale to China: The Lessons for Israel. Jerusalem Center for Public Affairs, 2002.
- CPCNEWS: **冷静**观察、沉着应付、韬光养晦、决不当头、有所作为. Forrás: http://theory.people.com.cn/n/2012/1028/c350803-19412863.html (Letöltés ideje: 2018. 08. 12.)
- EILAND, Michael D.: Military Modernization and China's Economy. Asian Survey, 1977, 17.12: pp. 1143-1157.
- FISHER, Richard D.: China's military modernization: building for regional and global reach. Greenwood Publishing Group, 2008.
- GHOSH, S. K.: China's Military Modernization Programme. China Report, 1978, 14.4: pp. 66-77.
- HÁDA Béla: Útban egy nemzeti álom felé? – Kína 2015. évi katonai stratégiája. Nemzet és Biztonság 2015/9. pp. 125-133.
- Information Office of the State Council Of the People's Republic of China. China's National Defense, 1998. http://www.china.org.cn/e-white/5/index.htm http://theory.people.com.cn/n/2012/1028/c350803-19412863.html (Letöltés ideje: 2018. 08. 12.)

- KISS Roland: Air-Sea Battle – A globális közös terekhez való hozzáférés hadműveleti koncepciója. Nemzet és Biztonság 2015/4. pp. 56-69.
- LIN, Chong-Pin: Chinese military modernization: perceptions, progress, and prospects. Security Studies, 1994, 3.4: pp. 718-753.
- LIU, Guoli: China rising: Chinese foreign policy in a changing world. Palgrave Macmillan, 2016.
- MEARSHEIMRE, John J.: The tragedy of great power politics. WW Norton & Company, 2001.
- SAICH, Tony: Governance and politics of China. Palgrave Macmillan, 2010.
- SHAMBAUGH, David L.: China's quest for military modernization. Asian Affairs: An American Review, 1979, 6.5: 295-309.
- Stockholm International Peace Research Institute: SIPRI Military Expenditure Database https://www.sipri.org/databases/milex http://theory.people.com.cn/n/2012/1028/c350803-19412863.html (Letöltés ideje: 2018. 08. 12.)
- The State Council Information Office of the People's Republic of China. China's Military Strategy. 2015. http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm http://theory.people.com.cn/n/2012/1028/c350803-19412863.html (Letöltés ideje: 2018. 08. 12.)
- The International Institute for Strategic Studies (IISS): Military Balance 1989. (2009) Asia and Australasia, The Military Balance, 89:1, pp. 145-179, DOI: 10.1080/04597228908460011
- The International Institute for Strategic Studies (IISS): Military Balance 1990. (2009) Asia and Australasia, The Military Balance, 90:1, pp. 148-181, DOI: 10.1080/04597229008460022
- The International Institute for Strategic Studies (IISS): Military Balance 1991. (2009) Asia and Australasia, The Military Balance, 91:1, pp. 149-184, DOI: 10.1080/04597229108460033
- The International Institute for Strategic Studies (IISS): Military Balance 1992. (2009) East Asia and Australasia, The Military Balance, 92:1, pp. 139-165, DOI: 10.1080/04597229208460044
- The International Institute for Strategic Studies (IISS): Military Balance 1993. (2009) East Asia and Australasia, The Military Balance, 93:1, pp. 146-172, DOI: 10.1080/04597229308460057
- The International Institute for Strategic Studies (IISS): Military Balance 1994. (2009) East Asia and Australasia, The Military Balance, 94:1, pp. 164-193, DOI: 10.1080/04597229408460070
- The International Institute for Strategic Studies (IISS): Military Balance 1995. (2009) East Asia and Australasia, The Military Balance, 95:1, pp. 168-198, DOI: 10.1080/04597229508460083

- The International Institute for Strategic Studies (IISS): Military Balance 1996. (2009) East Asia and Australasia, The Military Balance, 96:1, pp. 170-201, DOI: 10.1080/04597229608460097
- The International Institute for Strategic Studies (IISS): Military Balance 1997. (2009) East Asia and Australasia, The Military Balance, 97:1, pp. 164-198, DOI: 10.1080/04597229708460109
- The International Institute for Strategic Studies (IISS): Military Balance 1998. (2009) East Asia and Australasia, The Military Balance, 98:1, pp. 165-201, DOI: 10.1080/04597229808460121
- The International Institute for Strategic Studies (IISS): Military Balance 1999. (2009) East Asia and Australasia, The Military Balance, 99:1, pp. 171-209, DOI: 10.1080/04597229908460133
- The International Institute for Strategic Studies (IISS): Military Balance 2000. (2009) East Asia and Australasia, The Military Balance, 100:1, pp. 178-218, DOI: 10.1080/04597220008460145
- The International Institute for Strategic Studies (IISS): Military Balance 2001. (2009) East Asia and Australasia, The Military Balance, 101:1, pp. 172-213, DOI: 10.1080/04597220108460157
- The International Institute for Strategic Studies (IISS): Military Balance 2002. (2010) East Asia and Australasia, The Military Balance, 102:1, pp. 138-168, DOI: 10.1093/milbal/102.1.138
- The International Institute for Strategic Studies (IISS): Military Balance 2003. (2010) East Asia and Australasia, The Military Balance, 103:1, pp. 145-175, DOI: 10.1093/milbal/103.1.145
- The International Institute for Strategic Studies (IISS): Military Balance 2004. (2011) East Asia and Australasia, The Military Balance, 105:1, pp. 259-314, DOI: 10.1080/04597220500387662
- The International Institute for Strategic Studies (IISS): Military Balance 2005. (2011) East Asia and Australasia, The Military Balance, 105:1, pp. 259-314, DOI: 10.1080/04597220500387662
- The International Institute for Strategic Studies (IISS): Military Balance 2006. (2006) East Asia and Australasia, The Military Balance, 106:1, pp. 247-302, DOI: 10.1080/04597220600782887
- The International Institute for Strategic Studies (IISS): Military Balance 2007. (2007) East Asia and Australasia, The Military Balance, 107:1, pp. 331-384, DOI: 10.1080/04597220601181097
- The International Institute for Strategic Studies (IISS): Military Balance 2008. (2008) East Asia and Australasia, The Military Balance, 108:1, pp. 359-416, DOI: 10.1080/04597220801912879
- The International Institute for Strategic Studies (IISS): Military Balance 2009. (2009) Chapter Eight: East Asia and Australasia, The Military Balance, 109:1, pp. 363-424, DOI: 10.1080/04597220802709936

- The International Institute for Strategic Studies (IISS): Military Balance 2010. (2010) Chapter Eight: East Asia and Australasia, The Military Balance, 110:1, pp. 377-440, DOI: 10.1080/04597220903545874
- The International Institute for Strategic Studies (IISS): Military Balance 2011. (2011) Chapter Six: Asia, The Military Balance, 111:1, pp. 195-292, DOI: 10.1080/04597222.2011.559837
- The International Institute for Strategic Studies (IISS): Military Balance 2012. (2012) Chapter Six: Asia, The Military Balance, 112:1, pp. 205-302, DOI: 10.1080/04597222.2012.663215
- The International Institute for Strategic Studies (IISS): Military Balance 2013. (2013) Chapter Six: Asia, The Military Balance, 113:1, pp. 245-352, DOI: 10.1080/04597222.2013.757002
- The International Institute for Strategic Studies (IISS): Military Balance 2014. (2014) Chapter Six: Asia, The Military Balance, 114:1, pp. 201-296, DOI: 10.1080/04597222.2014.871879
- The International Institute for Strategic Studies (IISS): Military Balance 2015. (2015) Chapter Six: Asia, The Military Balance, 115:1, pp. 207-302, DOI: 10.1080/04597222.2015.996361
- The International Institute for Strategic Studies (IISS): Military Balance 2016. (2016) Chapter Six: Asia, The Military Balance, 116:1, pp. 211-306, DOI: 10.1080/04597222.2016.1127567
- The International Institute for Strategic Studies (IISS): Military Balance 2017. (2017) Chapter Six: Asia, The Military Balance, 117:1, pp. 237-350, DOI: 10.1080/04597222.2017.1271212
- The International Institute for Strategic Studies (IISS): Military Balance 2018. (2018) Chapter Six: Asia, The Military Balance, 118:1, pp. 219-314, DOI: 10.1080/04597222.2018.1416982
- TYLER, Patrick: China's Military Stumbles even as Its Power Grows. New York Times 1996 Dec. 3 https://www.nytimes.com/1996/12/03/world/china-s-military-stumbles-even-as-its-power-grows.html http://theory.people.com.cn/n/2012/1028/c350803-19412863.html (Letöltés ideje: 2018. 08. 12.)
- VÖRÖS Zoltán: Kína külpolitikai irányváltása a regionális tengerek vonatkozásában. Szakmai Szemle 2014/1. pp. 109-124.

BEDERNA ZSOLT

AZ ÁLTALÁNOS ADATVÉDELMI RENDELET ÉS AZ INFORMÁCIÓBIZTONSÁG KAPCSOLÓDÁSI PONTJAI

Előzmények

A technikai fejlődés alátámasztásaként az Eurostat[1] statisztikai szolgáltatására alapozva 2007 és 2018 közötti időszakban a termékek és szolgáltatások online vásárlási arányát, az elektronikus ügyintézés (ügyfélkapu) arányát, valamint az internetkapcsolattal rendelkező háztartások arányát vizsgáltam. Megállapítható, hogy mind az Európai Unió és Magyarország vonatkozásában az adott időszakban minden vizsgált jellemző tartósan növekedett:

	EU (28)			Magyarország		
	2008	**2017**	**Változás mértéke**	**2008**	**2017**	**Változás mértéke**
Termékek és szolgáltatások online vásárlási aránya	32%	57%	**56%**	14%	39%	**36%**
Elektronikus ügyintézés aránya (ügyfélkapu)	35%	49%	**71%**	28%	47%	**60%**
Internetkapcsolattal rendelkező háztartások aránya	60%	87%	**69%**	47%	82%	**57%**

1. ábra: Statisztikai jellemzők az Európai Unió és Magyarország vonatkozásában
Forrás: Eurostat

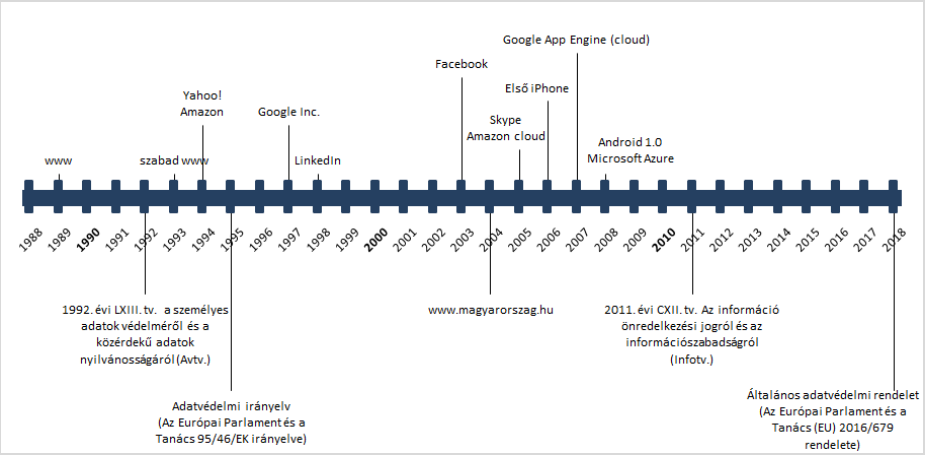
A technológiai változások és a személyes adatok megnövekedett kezelésére vonatkozó változások más, „kedvezőtlen" jelenségeket erősítettek fel. Az adatkezelési műveletek számbeli és jellegbeli változásával együtt megnövekedett a visszaélések száma az emberi hanyagság vagy tudás hiánya következtében. Nem kisebb jelentőségű veszélyforrás a belső szabályozatlanság, illetve a szükséges technikai kontrollok nem megfelelősége vagy annak teljes hiánya[2].

[1] http://ec.europa.eu/eurostat (Letöltés ideje: 2018. 03. 28.)

[2] Ponemon Institute LLC: The Need for a New IT Security Architecture: Global Study on the Risk of Outdated Technologies, 2017. 02. https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/ponemon-institute-security-study-outdated-technology-risks.pdf. (Letöltés ideje: 2018. 03. 21.); Ponemon Institute LLC: The Need for a New IT Security Architecture: Global Study 2017. 01. https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/ponemon-security-study.pdf. (Letöltés ideje: 2018. 03. 21.);

Az említett pontokon túlmenően további problémát jelent, hogy a felgyorsuló technológiai fejlődés és a globalizáció nemcsak az adatgyűjtést végzőket, hanem a jogalkotókat is folyamatosan új kihívások elé állítja a személyes adatok védelme tekintetében. A jogalkotók jellemzően a technológia fejlődését utólag reagálják le. Ezt a tényt támasztja alá, hogy „*a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról*” elnevezésű Európai Parlament és a Tanács 95/46/EK irányelve 1995. október 24-én lépett hatályba, és az adatvédelmi kérdésekkel újfent 2012-ben kezdtek el foglalkozni. Másfelől az irányelvet a magyar jogszabályi környezetbe az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) implementálta.

A jogszabály technológiai elavultsága (2. ábra) mellett egy következő probléma a jogszabály irányelv-jellegéből adódott, mely szerint az egyes tagállami törvényeket az előírtak alapján, az eltérési lehetőségek figyelembevétele mellett kellett megalkotni. (Egy irányelvet minden esetben át kell emelni a tagállami jogrendszerbe.) Ennek velejárója, hogy az egyes értelmezésbeli, szövegezésbeli és attitűdbeli különbségek következtében a tagállamokban eltérő követelmények léptek életbe. Az olykor jelentős mértékű tagállami eltérések az uniós polgárok számára nem ugyanazt a garanciát biztosították, valamint a gazdasági társaságoknak nem egységes követelményeket írtak elő. Ezek figyelembevételével kijelenthető, hogy tulajdonképp ezek az egységes piac ellen dolgoztak.



2. ábra: A jelentősebb technológiai fejlődés és a jogszabályok szubjektív, kronologikus szemléltetése
(saját szerkesztés)

Ponemon Institute LLC: 2017 Cost of Data Breach Study, 2017. 06. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN. (Letöltés ideje: 2018. 01. 15.)

A technológiai fejlődéssel párhuzamosan a kiberbűnözők stratégiát váltottak, a Trend Micro Inc. által, az Általános adatvédelmi rendeletről való egyeztetések megkezdésekor, azaz 2012-ben készített felmérés szerint a „Hacking as a service" már javában élő szolgáltatást jelentett a feketepiacon[3]. A jelentés szerint egy órányi DDoS támadás ellenértéke mindössze $10 volt. A hackertámadások és más úton kivitelezett adatszivárgást erősítette az a tény, hogy a (vállalati) bizalmas adatok, különösképp a személyes adatok jelentősége és értéke is fokozódott mind az adatvagyon valós tulajdonosa, mind a támadók részéről egyaránt.

Az IBM Security által szponzorált, 2017. évre vonatkozó felmérés[4] szerint a vizsgált vállalatok körében 2.600 és 100.000 darab rekord közé tehető az egy adatvédelmi incidens esetén kompromittálódó rekordok száma. Globális átlagban ez 24.089 darab személyes adatot tartalmazó rekordot jelentett egy adatszivárgási esemény esetén. Az incidensek során érintett adatrekordokat csoportosítva a csoportonkénti átlagos teljes költség a következőképp alakult: 10.000 alatt $1,9 millió, 10.000 és 25.000 között $2,8 millió, 25.001 és 50.000 között $4,6 millió, valamint 50.0000 fölött $6,3 millió. Ezen túlmenően a felmérés során számos szektor érintettségét vizsgálták (pl. közszféra, energetika, pénzügyi és egészségügy stb.), amely szerint az egy adatvédelmi rekord esetén a becsült teljes költség az adott szervezet számára $71 (közszféra) és $380 (egészségügy) intervallumra tehető.

Magyarországi viszonylatban az adatvédelmi incidensek vonatkozásában érdemben rendelkezésre álló hivatalos statisztikai forrást a NAIH (Nemzeti Adatvédelmi és Információszabadsági Hatóság)[5] éves beszámolói[6] jelentenek, melyet az alábbi ábrával foglaltam össze – megkülönböztetve a jogellenesség megállapításával és megállapítása nélkül végződő tényleges vizsgálatokat. (A 2012. évre vonatkozó kiemelkedő adatok alapját az adatvédelmi ombudsmantól átvett eljárások jelentették.)

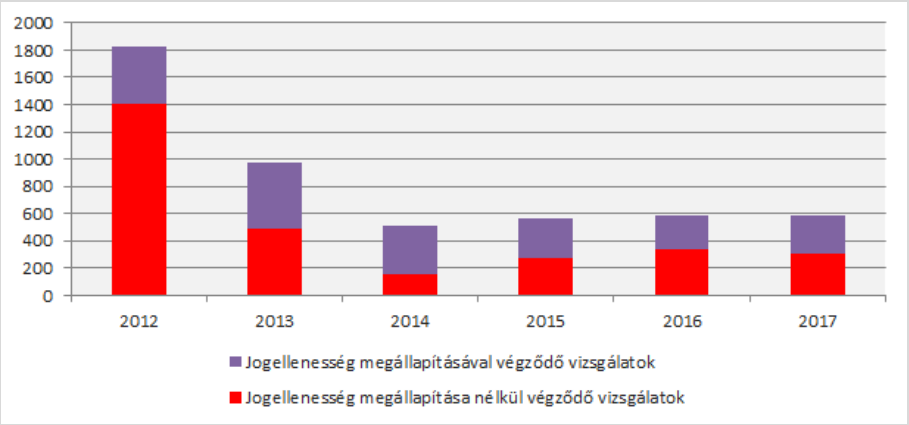
---

3 Trend Micro Inc.: Russian Underground 101, 2012. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf. (Letöltés ideje: 2018. 01. 14.)

4 A felmérés 13 országban, illetve régióban 419 vállalat részvételével készítették. Az országok/régiók a következőek voltak: India, Közel-Kelet (az Egyesült Arab Emirátus és Szaúd Arábia országokat beleértve), Egyesült Államok, Brazília, Franciaország, Németország, Kanada, Egyesül Királyság, Japán, Ausztrália, Olaszország, Dél Afrikai Köztársaság, Délkelet-ázsiai Nemzetek Szövetsége régió (Szingapúr, Indonézia, Fülöp Szigetek és Malajzia országokat beleértve).

5 http://naih.hu/

6 http://naih.hu/naih-eves-beszamoloi.html



3. ábra: A NAIH adatvédelmi vizsgálatai 2012-2017 között
(saját szerkesztés a NAIH éves beszámolók alapján[7])

Általános adatvédelmi rendelet

E tényeket realizálva, az Európai Unió illetékes szervei 2012-ben elkezdték kidolgozni az új adatvédelmi szabályozás alapjait. A többkörös egyeztetések eredményeként 2016. április 27-én hatályba lépett *„az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (Általános adatvédelmi rendelet)”*, azaz GDPR (General Data Protection Regulation) mintegy kétéves, a felkészülést segítő türelmi idővel. Ennek megfelelően a rendeletben megszövegezett követelményeket 2018. május 25-től kell alkalmazni.

Az új szabályozással egy szilárd és az eddiginél következetesebb uniós adatvédelmi keret ellenében egyértelmű elvárásokat támasztottak, úgymint erős kikényszeríthetőség, a természetes személyek számára a saját személyes adataik

[7] NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2012. évi tevékenységéről, 2013. http://naih.hu/files/NAIH_BESZaMOLo_2012_net3.pdf. (Letöltés ideje: 2018. 12. 20.) p. 9.
NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2013. évi tevékenységéről, 2014. http://naih.hu/files/NAIH-beszamolo2013--MID-RES.pdf. (Letöltés ideje: 2018. 12. 20.) p. 10
NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2014. évi tevékenységéről, 2015. http://naih.hu/files/NAIH-2014-eves-beszamolo-magyar-MR.pdf. (Letöltés ideje: 2018. 12. 20.) p. 10
NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2015. évi tevékenységéről, 2016. http://naih.hu/files/NAIH-BESZ-MOL--2015-MID-RES.pdf. (Letöltés ideje: 2018. 12. 20.) p. 11
NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2016. évi tevékenységéről, 2017. http://naih.hu/files/NAIH-BESZ-MOL--2016_Mid-Res.pdf. (Letöltés ideje: 2018. 12. 20.) p. 8
NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2017. évi tevékenységéről, 2018. http://naih.hu/files/NAIH-BESZAMOLO-2017-mid-res.pdf. (Letöltés ideje: 2018. 12. 20.) p. 9

feletti rendelkezés elősegítése, valamint minden szereplő számára a jogbiztonság és a működési biztonság fokozása. Ennek értelmében a tárgyi és területi hatályban szereplő feltételek teljesülése esetére határoz meg elvárásokat, úgymint jogszerűség, adatkezelési elvek, az érintettek jogai, szervezési és technológiai kötelezettségek, valamint általános jellegű információbiztonsági kontrollok és elvárások vonatkozásában. Az adatkezelők és adatfeldolgozók számára a nagy hívó szó a 83. cikkben meghatározott szankció lehetséges maximális mértéke lett.

Tárgyi és területi hatály

Az Általános adatvédelmi rendelet tárgyi hatálya (2. cikk) előírja, hogy „*a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére kell alkalmazni, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni*". Máshogy fogalmazva, a rendelet alkalmazása kiterjed az informatikai rendszerekben és a papíralapon kezelt személyes adatok kezelésére egyaránt.

A személyes adatok köréhez és jellegéhez a rendelet fogalom-meghatározása (4. cikk) nyújt támpontot. Ez alapján a személyes adat „*azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ*. Továbbá *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"*. A személyes adatok körét tovább szofisztikálja a 9. cikk (1) bekezdés, amely definiálja a különleges jellegű személyes adatokat. Különleges jellegű személyes adatnak számít „*a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok"*.

Ezzel összhangban áll az Egyesült Államok Szövetségi Törvénykönyvében szereplő definíció, azonban nem beszélhetünk teljes körű egyezésről, ennek következtében véleményem szerint a két fogalom nem alkalmazható egymás szinonimájaként. A 2. cím Code of Federal Regulations 200.79§ szerint a személyazonosításra alkalmas információ (Personally Identifiable Information – PII) *„minden olyan egyedi vagy kombinált információt magában foglal, amellyel egy személy beazonosítható vagy nyomon követhető. Egyes információk publikusan elérhető forrásban fellelhetőek, például telefonkönyv, publikus weboldal és egyetemi listák. E kategóriába tartozó információk publikus személyazonosításra alkalmas információnak tekintendők, és például a tartalma lehet a kereszt- és vezetéknév, cím, munkahelyi telefonszám, e-mail cím, otthoni telefonszám és általános oktatási bizonyítványok. A definíció nem kötődik egy adattípushoz vagy technológiához, inkább minden esetben meg kell vizsgálni az aktuális adatokat, az érintett személy vonatkozásában a specifikus kockázatokat. A személyazonosításra nem alkalmas információ bármikor személyazonosításra alkalmas információvá válhat, amennyiben a publikusan vagy bármely adathordozón vagy egyéb forrásból elérhető információval kombinálva alkalmassá válik az érintett személy beazonosítására.*"

Az Általános adatvédelmi rendelet területi hatályaként a 3. cikk szerint azok az adatkezelők vagy adatfeldolgozók szerepelnek, akik az Európai Unió területén tevékenységi hellyel rendelkeznek, függetlenül az adatkezelési tevékenységük célterületétől, vagy akik az Európai Unió területén nem rendelkeznek tevékenységi hellyel, de az adatkezelési tevékenységük az Unióban tartózkodó érintettekre vonatkozik.

Ismét a 4. cikkből merítve, adatkezelőnek minősül az „a *természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza*, illetve adatfeldolgozónak minősül *az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel*. E meghatározások értelmezéséhez egy további fogalom, az adatkezelés definícióját szükséges megvizsgálni, amely szerint adatkezelésnek minősül *a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége"*. Ilyen műveletnek minősül például a rögzítés, gyűjtés, tárolás, módosítás, lekérdezés, betekintés, korlátozás, törlés, valamint a közlés, továbbítás és terjesztés egyaránt, nem beszélve a több adatbázis összekapcsolásáról és a profilozásról.

A személyes adatok kezelésére vonatkozó elvek

Az adatkezelési műveletekre vonatkozóan alapvető elveket, illetve az érintettek számára alapvető jogokat határoz meg a rendelet, melyeknek az esetleges adatvédelmi incidensek bekövetkezése vagy egy adatvédelmi audit esetén a kirótható szankciók mértékének meghatározásában is jelentősége van. A személyes adatok kezelésére vonatkozó elveket az 5. cikk határozza meg, melyek:

- „Jogszerűség, tisztességes eljárás és átláthatóság" – A személyes adatokra vonatkozó adatkezelést jogszerűen, tisztességesen és az érintettek számára átlátható módon kell végezni.
- „Célhoz kötöttség" – A személyes adatok gyűjtése csak előre meghatározott, egyértelmű és jogszerű célból történjen.
- „Adattakarékosság" – Az adatkezelési tevékenység csak és kizárólag a szükséges személyes adatokra korlátozódjon.
- „Pontosság" – Biztosítani kell az adatkezelési tevékenységben érintett személyes adatok naprakészségét, és amennyiben az adott személyes adat megjelenik más szervezeti vagy adatfeldolgozói adatbázisban, akkor annak helyesbítését vagy törlését is végre kell hajtani.
- „Korlátozott tárolhatóság" – A személyes adatok tárolását olyan formában szükséges megvalósítani, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.
- „Integritás és bizalmas jelleg" – A személyes adatok kezelése során megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítani kell a személyes adatok biztonságát a bizalmasság, sértetlenség és rendelkezésre állás tekintetében.

Az adatkezelés jogszerűsége

Az adatkezelő és az adatfeldolgozó a tevékenysége során végzett adatkezelési műveletekre vonatkozóan a fenti felsorolásban szereplő elvek közül a jogszerűség az egyik legfontosabb kitétel. A 6. cikk szerint az adatkezelés akkor tekintendő jogszerűnek, ha:

- az érintett hozzájárulását adta,
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél,
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges,
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges,
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges,
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Az utolsó kitétel nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre. Továbbá az adatkezelő és az adatfeldolgozó felelős a felsorolásban szereplő elvek betartásáért, továbbá képesnek kell lennie e megfelelés igazolására. Ez pedig maga az „elszámoltathatóság” elve.

Az érintettek jogai

Az adatkezelési műveletekre vonatkozó alapvető elvek kiegészítéseként a rendelet igen széles körben határozza meg az érintettek jogait:

- Tájékoztatáshoz való jog (12. cikk) – Az „Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések” a közérthető adatvédelmi magyarázathoz való jogról rendelkezik olyan formán, hogy az adatkezelő minden fellépő tájékoztatási kötelezettsége esetén tömör, átlátható, érthető és könnyen hozzáférhető formában, írásban, elektronikus formában vagy szóban megadja az érintett kilétének megállapítását követően;
- Az érintett hozzáférési joga (15. cikk) – Az érintett kérésére az adatkezelő tájékoztatja, hogy személyes adatainak kezelése folyamatban van-e. Pozitív válasz esetén jogosult a rá vonatkozó személyes adatokhoz és a következő információkhoz hozzáférést kapni;
- A helyesbítéshez való jog (16. cikk) – Az érintett kérésére az adatkezelőnek módosítania kell az érintettre vonatkozó pontatlan személyes adatokat;
- A törléshez való jog (17. cikk) – Az érintett kérésére az adatkezelőnek törölni kell az érintettre vonatkozó személyes adatokat, amennyiben a meghatározott feltételek fennállnak;

- Az adatkezelés korlátozásához való jog (18. cikk) – Az érintett kérésére az adatkezelő korlátozza az adatkezelést, amennyiben a meghatározott feltételek fennállnak;
- Az adathordozhatósághoz való jog (20. cikk) – Az érintett jogosult, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, valamint továbbítsa azt egy másik adatkezelőnek;
- A tiltakozáshoz való jog (21. cikk) – Az érintett jogosult a közérdekű adatkezelés vagy a jogos érdek jogalapú adatkezelések ellen tiltakozni;
- Az adatvédelmi incidensről való értesülés joga – Az incidensről való értesülést a 33. és a 34 cikk írja elő, melyek alapján az adatvédelmi incidenst be kell jelenteni a felügyeleti hatóságnak, valamint az előírt feltételek teljesülése esetén tájékoztatnia kell az érintetteket;
- A felügyeleti hatóságnál történő panasztételhez való jog (77. cikk) – Minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál, ha a személyes adatait kezelő adatkezelő vagy adatfeldolgozó véleménye szerint megsérti a jogait;
- A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog (78. cikk) – Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben;
- Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog (79. cikk) – Minden érintett bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak nem megfelelő kezelése következtében megsértették a jogait;
- A kártérítéshez való jog és a felelősség (82. cikk) – Minden olyan személy, aki az előírt kötelezettségek megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult;
- A személyes adatok kezelése és a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog (85. cikk) – Minden tagállam kötelezettsége, hogy a nemzeti jogszabályban összeegyezteti a személyes adatok e rendelet szerinti védelméhez való jogot a véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal.

Szervezési és technikai kötelezettségek

A rendelet a személyes adatok kezelésére vonatkozó elvek és az érintettek jogainak biztosítása végett szervezési és technikai kötelezettségek (kontrollok) bevezetését és fenntartását írja elő, melyeket több szempontból is lehetséges kategorizálni. Egyrészt jellegük szerint szervezési és technikai kontrollok különböztethetőek meg. Másrészt egyes kontrollok iránti igényt a rendelet explicit megfogalmazza, azaz előírja, míg más kontrollok bevezetése az adott adatkezelő és adatfeldolgozó szuverén döntése, azaz opcionális jellegű.

A 24. cikkel (Az adatkezelő feladatai) és a 25. cikkel (Beépített és alapértelmezett adatvédelem) összhangban a 32. cikk (Az adatkezelés biztonsága) szerint „*az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a*

megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre". Az előálló kontrollok származhatnak az adatvédelmi hatásvizsgálat vagy úgymond a hagyományos jellegű információbiztonsági kockázatelemzés eredményeképp – és vonatkozhatnak a fizikai, adminisztratív és logikai síkra egyaránt. Mindezzel a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét kell megvalósítani. Ezen túlmenően az implementált kontrollok hatékonyságáról rendszeres teszteléssel kell megbizonyosodni. A meghatározó jellegű szervezési és technikai kötelezettségeket az alábbiakban foglaltam össze:

A szervezési kötelezettségek tekintetében az adatkezelési tevékenységek a 30. cikk szerinti nyilvántartása az egyik legfontosabb követelménypont. Ez alapján minden adatkezelő és adatfeldolgozó az előírt tartalmi kötelezettségeknek megfelelően – a meghatározott feltételek teljesülése esetén – az adatkezelési műveletekről nyilvántartást hoz létre és tart fenn.

A felkészülés során, párhuzamosan a nyilvántartás készítésével a beépített és alapértelmezett adatvédelem (25. cikk) szerint a meglévő adatbázisokat és egyben az adatkezeléseket felül kell vizsgálni, azaz adatbázis-tisztítást kell végrehajtani, amellyel biztosítható, hogy a továbbiakban csak a szükséges adatok szerepeljenek.

Egy további nyilvántartási kötelezettség az adatvédelmi incidensekre vonatkozik. A nyilvántartás vezetésén túlmenően a hatóság felé bejelentési, míg az érintettek felé tájékoztatási kötelezettsége adódik „Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak" (33. cikk) és „Az érintett tájékoztatása az adatvédelmi incidensről" (34. cikk) szerint.

Különösen új technológiák alkalmazó, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, amely valószínűsíthetően magas kockázattal jár az érintetti jogok gyakorlására, adatvédelmi hatásvizsgálatot kell lefolytatni az „Adatvédelmi hatásvizsgálat" (35. cikk) szerint.

A hatásvizsgálattal összhangban, amennyiben az adatkezelés valószínűsíthetően magas kockázattal jár, az adatkezelő az illetékes hatósággal az adatkezelési művelet megkezdése előtt egyeztet az „Előzetes konzultáció" (36. cikk) szerint.

Az adatkezelő és az adatfeldolgozó a meghatározott esetekben a meghatározott követelmények figyelembevétele mellett adatvédelmi tisztviselőt nevez ki „Az adatvédelmi tisztviselő kijelölése" (37. cikk) szerint.

Iparági specialitások figyelembevétele mellett arra vonatkozóan ajánlás dolgozható ki a „Magatartási kódexek" (40. cikk) szerint.

Az Unión kívüli állam felé a személyes adatokra vonatkozó adattovábbítás jellegét „A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása" (V. fejezet: 44-50. cikk) szerint kell megvalósítani.

Az érintettek tájékoztatásához az adatkezelő és az adatfeldolgozó az érintett részére a személyes adatok kezelésére vonatkozóan a 13. és a 14. cikkben említett, az érintetti jog gyakorlásához a 15–22. cikkekkel összhangban és a 34. cikk szerint a bekövetkezett adatvédelmi incidenssel kapcsolatosan valamennyi információt megadja.

A hatásvizsgálat eredményeképp további operatív szintű szervezési kontrollok iránti igények fogalmazódhatnak meg. Továbbá a rendelet a 25. cikkben a beépített és alapértelmezett biztonságról rendelkezik. Minthogy a szervezet működési felépítése, működési folyamatai és működési környezete dinamikus jelleggel változik, ezért a változásokat az előírtakkal összhangban kell kivitelezni, amellyel a változásmenedzsment iránti igény fogalmazódik meg. Az adatkezelő és az adatfeldolgozó a rendeletnek való megfelelését a „Tanúsítás" (42. cikk) szerint érheti el.

A technikai kötelezettségek tekintetében kötelező jellegű funkcionalitásnak tekintendő az érintetti jogokra vonatkozó joggyakorlás technikai megvalósítása, úgymint a helyesbítési, törlési, hozzáférési, az adatkezelés korlátozásához, adathordozhatósághoz való jog. „Az adatkezelés biztonsága" (32. cikk) alapján kötelező jellegű információbiztonsági kontrollokat ír elő a személyes adatok titkosítása, álnevesítése (aninomizálása), hozzáférések kezelése formájában.

A 32. cikk továbbá előírja a kockázatarányos védelem megvalósítását a hatásvizsgálat vagy információbiztonsági kockázatelemzés eredményeképp előálló szervezési és technikai kontrollok formájában.

Szankciók

A jogszabályi előírások be nem tartására a 83. cikk kétféle esetet különböztet meg. A kisebb kihágások esetén legfeljebb 10.000.000 EUR összegű közigazgatási bírság vagy vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb két százalékát kitevő összeg szabható ki, amelyek közül a magasabb összeget kell figyelembe venni. A 83. cikk (4) szerint e kategóriába tartozó témakörök:

- Az adatkezelők és adatfeldolgozók tekintetében
    - A gyermek hozzájárulására vonatkozó feltételek az információs társadalommal összefüggő szolgáltatások vonatkozásában (8. cikk),
    - Az azonosítást nem igénylő adatkezelés (11. cikk),
    - Az általános kötelezettségek (25-39. cikk: A beépített és alapértelmezett adatvédelem; A közös adatkezelők; Az Unióban tevékenységi hellyel nem rendelkező adatkezelők vagy adatfeldolgozók képviselői; Az adatfeldolgozó, az adatkezelő vagy az adatfeldolgozó irányítása alatt végzett adatkezelés; Az adatkezelési tevékenységek nyilvántartása; Az együttműködés a felügyeleti hatósággal),
    - Az adatbiztonság (32-34. cikk: Az adatkezelés biztonsága; Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak;, Az érintett tájékoztatása az adatvédelmi incidensről),

- Az adatvédelmi hatásvizsgálat és előzetes konzultáció (35-36. cikk: Adatvédelmi hatásvizsgálat; Előzetes konzultáció),
- Az adatvédelmi tisztviselő (37-39. cikk: Az adatvédelmi tisztviselő kijelölése; Az adatvédelmi tisztviselő jogállása; Az adatvédelmi tisztviselő feladatai), valamint
- A Magatartási kódexek és tanúsítás (42-43. cikk: Tanúsítás; Tanúsító szervezetek).

- A tanúsító szervezet tekintetében a Magatartási kódexek és tanúsítás (42-43. cikk: Tanúsítás; Tanúsító szervezetek).
- Az ellenőrző szervezet tekintetében a (41. cikk (4): A jóváhagyott magatartási kódexeknek való megfelelés ellenőrzése).

Súlyosabb kihágás esetén legfeljebb 20.000.000 EUR összegű közigazgatási bírság, továbbá a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb négy százalékát kitevő összeg szabható ki, amelyek közül a magasabb összeget kell kiszabni. A 83. cikk (5) és (6) bekezdése szerint e kategóriába tartozó témakörök:

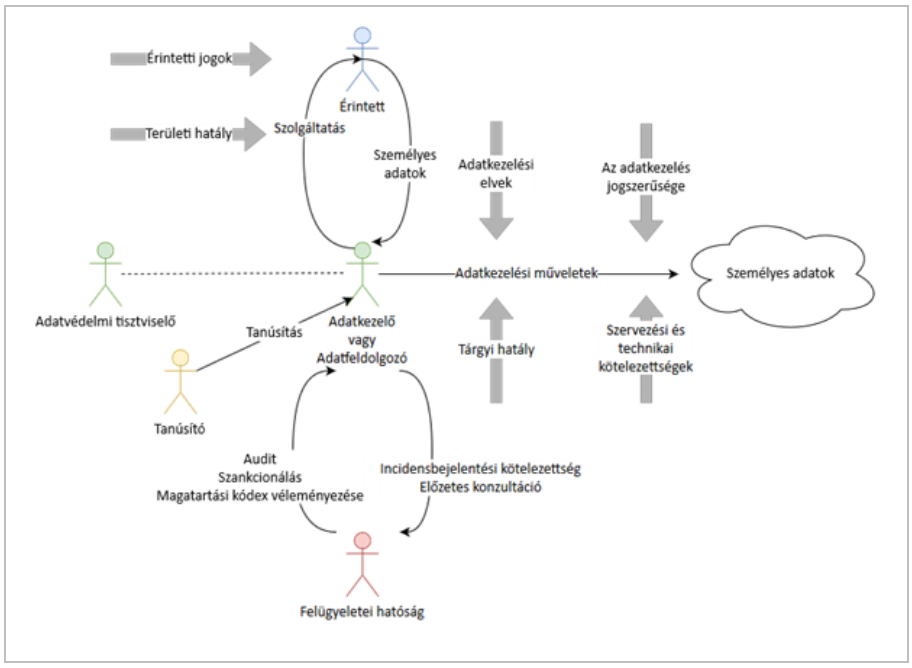
- A felügyeleti hatóság 58. cikk (2) bekezdése szerinti utasításának, illetve az adatkezelés átmeneti vagy végleges korlátozására vagy az adatáramlás felfüggesztésére vonatkozó felszólításának be nem tartása vagy az 58. cikk (1) bekezdését megsértve a hozzáférés biztosításának elmulasztása, valamint
- Az adatkezelés elvei – ideértve a hozzájárulás feltételeit – az 5., 6., 7. és 9. cikknek megfelelően,
- Az érintettek jogai a 12–22. cikknek megfelelően,
- A személyes adatoknak harmadik országbeli címzett vagy nemzetközi szervezet részére történő továbbítása a 44–49. cikknek megfelelően,
- Az elfogadott tagállami jog szerinti kötelezettségek megsértése.

Az egyes kihágások esetére kiszabott közigazgatási bírságok ellenében határozott elvárás, hogy az újabb kihágást okozó tevékenységre vonatkozóan visszatartó erőt jelentsen. További elvárás a szankció mértékének arányossága, tekintettel a jogsértést okozó adatkezelés jellegét, célját, érintett személyes adatok kategóriáit, valamint az érintettek számát és az általuk elszenvedett kár mértékét. Ugyanígy befolyásoló tényező a jogsértés szándékolt vagy nem szándékolt jellege, a hatóság felé történő incidens-bejelentés megléte, valamint a korábban, az incidens észlelése alatt és az azt követően végzett technikai és szervezeti intézkedések jellege. Továbbá növeli a szankció mértékét, ha az adatkezelő vagy az adatfeldolgozó visszaeső, notórius jogsértő.

Adatvédelmi irányítás rendszer

A korábban tárgyalt információkat alapul véve kialakítható az adatvédelem modellje (4. ábra). Meghatározó eleme a személyes adatok kezelésére vonatkozó elvek, az adatkezelés jogszerűsége, az érintettek jogai, az adatkezelők és adatfeldolgozók feladatai, valamint a szervezeti és technikai kötelezettségek. Ezen túlmenően a rendelet 42. cikke szerint a szervezet adatkezelési működését egy

független tanúsító-szervezet által tanúsítani lehetséges. A tanúsítás lefolytatásához a Bureau Veritas tanúsító szervezet az ISO szabványoknak megfelelő formában még a 2017. év során elkészítette a technikai sztenderd tervezetét[8].



4. ábra: Adatvédelmi modell
(saját szerkesztés)

Ahhoz, hogy a felvázolt modell Adatvédelmi irányítási rendszerré (ADIR) váljon, definiálni szükséges a működtetéséért felelős személyét. A 37. cikk (Az adatvédelmi tisztviselő kijelölése) azokat az eseteket taglalja, amelyek esetén az adatkezelőknek és adatfeldolgozóknak adatvédelmi tisztviselőt kell kijelölniük. A rendelet által meghatározott esetek az alábbiak:

- Közhatalmi vagy közfeladatot ellátó szerv esetén (kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságok),
- Az érintettek rendszeres és szisztematikus, nagymértékű megfigyelése esetén,
- Fő tevékenységei a személyes adatok 9. cikk szerinti különleges kategóriáinak és a 10. cikk szerinti büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelése.

[8] Bureau Veritas: Technical Standard related to personal data protection in compliance with the regulation (EU) 2016/679, 2017. http://www.bureauveritas.hu/4856710d-67db-4b65-918b-7ac912b335d1/Data+Protection_Technical+standard_Bureau+Veritas.pdf?MOD=AJPERES. (Letöltés ideje: 2018. 02. 15.)

A 38. cikk (Az adatvédelmi tisztviselő feladatai) deklarálja az adatvédelmi tisztviselő feladatait:

- Tájékoztat és szakmai tanácsot ad az adatkezelő, az adatfeldolgozó, valamint az adatkezelést végző alkalmazottak számára a Rendelet, további uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.
- Ellenőrzi az adatvédelmi jogszabályi kötelezettségek, továbbá a személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést. Ide értendő a feladatkörök kijelölése, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelése és képzése, valamint a kapcsolódó auditok egyaránt.
- Az adatvédelmi hatásvizsgálat témakörében szakmai tanácsot ad, továbbá nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését.
- Együttműködik a felügyeleti hatósággal.
- Az adatkezeléssel összefüggő ügyekben (pl. a 36. cikkben említett előzetes konzultáció) kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

A 37. cikk (6) bekezdése szerint adatvédelmi tisztviselő jogállása szerint lehet belső munkavállaló vagy külső fél, ugyanakkor a 37. cikk (1) bekezdése alapján az adatvédelmi tisztviselő kijelölése nem minden esetben kötelező jellegű. Amennyiben ez a tényállás áll fenn, akkor is szükségszerű egy Adatvédelmi felelős kijelölése. Az alábbi táblázat a legfőbb feladatokat foglalja össze a 38. cikkben meghatározott listát további feladatokkal kiegészítve. A kapcsolattartói feladatok részét képezi az érintettek részéről érkező törlési igény regisztrálása, a feladat elvégzésének számonkérése, valamint a törlés megtörténtéről az érintett tájékoztatása. Természetesen a törlési igény csak abban az esetben teljesíthető, amennyiben erre a jogalap lehetőséget biztosít (pl. hozzájárulás esetén).

Feladat	Adatvédelmi tisztviselő/ Adatvédelmi felelős	Adatkezelő/ Adatfeldolgozó üzleti egységei	Jogi osztály, jogtanácsos	Vezetőség
Adatvédelmi szabályzat és adatvédelmi tájékoztatók elkészítése és felülvizsgálata	Felelős Elszámoltatható	Konzultáló	Konzultáló	Támogató
Adatkezelési műveletek nyilvántartásának elkészítése, karbantartása	Elszámoltatható	Felelős	Konzultáló	Támogató
Tájékoztat és szakmai tanácsot ad az adatkezelő, az adatfeldolgozó, valamint az adatkezelést végző alkalmazottak számára a Rendelet, további uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.	Felelős Elszámoltatható	Konzultáló	Konzultáló	Támogató
Ellenőrzi az adatvédelmi jogszabályi kötelezettségek, továbbá a személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést. Ide értendő a feladatkörök kijelölése, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelése és képzése, valamint a kapcsolódó auditok egyaránt.	Felelős Elszámoltatható	Konzultáló	Konzultáló	Támogató
Az adatvédelmi hatásvizsgálat témakörében szakmai tanácsot ad, továbbá nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését.	Felelős Elszámoltatható	Konzultáló	Konzultáló	Támogató
Együttműködik a felügyeleti hatósággal.	Felelős Elszámoltatható	Konzultáló	Konzultáló	Támogató
Az adatkezeléssel összefüggő ügyekben (pl. a 36. cikkben említett előzetes konzultáció) kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.	Felelős Elszámoltatható	Konzultáló	Konzultáló	Támogató
Az érintettől érkező törlési igény feldolgozása	Elszámoltatható	Felelős	Konzultáló	Támogató
Az érintettől érkező tájékoztatási igény	Felelős Elszámoltatható	Konzultáló	Konzultáló	Támogató

5. ábra: Feladatok és felelősségek
(saját szerkesztés)

Információbiztonsági irányítási rendszer

Az Információbiztonsági irányítási rendszer (IBIR) kiépítésére és működtetésére számos megközelítés létezik. Az IBIR alapvető eleme az azt meghatározó folyamatok kialakítása és fenntartása, mely az információbiztonsági felelős felelőssége.

Annak eldöntése, hogy mi képezze a keretrendszer részét, kiváló támpontot nyújt az MSZ ISO/IEC 27001:2014 szabvány A melléklete. Az információbiztonsági szervezetre és az információbiztonsági szabályokra vonatkozó követelmények teljesítésével a keretrendszer működéséhez feltétlen szükséges folyamatokat határozhatunk meg. Ezen túlmenően az elvárt szintű információbiztonság eléréséhez és fenntartásához szükséges további adminisztratív, fizikai és technikai (logikai) kontrollok kiválasztása összességében a kockázatelemzési folyamat eredményeképp áll elő. A kontrollok az adminisztratív, logikai és fizikai síkon egyaránt szolgálhatják az elrettentés, megelőzés, javítás, visszanyerés, észlelés, kompenzálás megvalósítását:

	Adminisztratív	**Fizikai**	**Technikai**
Elrettentő		- Kerítés	
Megelőző	- Biztonsági politika - Szerepkörök elkülönítése - Oktatás	- Zár - Biztonsági őr - Biometrikus vagy kártyás beléptető	- Intrusion Prevention System - Tűzfal - Titkosítás - UPS[9]
Javító	- Patch menedzsment		- Képfájlból való visszatöltés
Visszanyerés			- Adatmentés és visszaállítás - HA[10] biztosítása
Észlelő	- Feladatok rotálása - Auditálás	- Kamerás megfigyelés - Mozgásérzékelő	- Intrusion Detection System - Security Incident and Event Management
Kompenzáló	- Üzletmenet-folytonossági terv végrehajtása		

6. ábra: Példa kontrollok
Saját szerkesztés

[9] UPS – szünetmentes tápellátás
[10] HA – high availability – magas szintű rendelkezésre állás

Az MSZ ISO/IEC 27001:2014 szabvány A mellékletében szereplő követelmények, azaz témakörök az alábbiak (a követelménypontok kifejtésétől a beszédes jellegük miatt eltekintek)[11]:

- A.5 – Információbiztonsági szabályok,
- A.6 – Az információbiztonság szervezete,
- A.7 – Emberi erőforrás biztonsága,
- A.8 – Vagyonelemek kezelése,
- A.9 – Hozzáférés-felügyelet,
- A.10 – Titkosítás,
- A.11 – Fizikai és környezeti biztonság,
- A.12 – Az üzemelés biztonsága,
- A.13 – A kommunikáció biztonsága,
- A.14 – Rendszerek beszerzése, fejlesztése és karbantartása,
- A.15 – Szállítói kapcsolatok,
- A.16 – Az információbiztonsági incidensek és javítások kezelése,
- A.17 – A működésfolytonosság biztosításának információbiztonsági vonatkozásai,
- A.18 – Megfelelés.

Az IBIR működtetése a PDCA (plan – tervezés, do – cselekvés, check – ellenőrzés, act – beavatkozás) szemléletet követi. A kockázatok elemzéséből és a felismert kockázatok kezelésére kiválasztott kontrollok tervezéséből, bevezetéséből és működtetéséből, valamint a visszamérésből áll. Mindezen tevékenységek központjában a kezelt adatvagyon áll. Az üzleti szolgáltatások a szervezet adatvagyonára, az informatikai szolgáltatások az adatvagyonnal kapcsolatos adatkezelési műveletekre épülnek, míg az információbiztonság az adatvagyon védelmét szolgálja.

Az IBM Analytics által rendelkezésemre bocsátott információk szerint az adatvagyon vonatkozásában egy 2015. évben készített felmérés során a következő megállapításokat tették:

- Az adatok 5 százaléka a szabályozásokhoz kapcsolódó adatokat,
- Az adatok 1 százaléka jogi megfeleléshez szükséges adatokat,
- Az adatok 25 százaléka üzletileg értékes adatokat, valamint
- A maradék 69 százalék funkció nélküli, értéktelen vagy épp redundánsan tárolt adatokat takar.

Az információbiztonság keretrendszerének legmeghatározóbb alapeleme a megfelelő felsővezetői támogatás megléte. A kontrollok jellegére, minőségére vonatkozóan az igények javarészt az üzleti folyamatokból származnak. Ugyanakkor az informatikai rendszerek és szolgáltatások is befolyásolhatják az üzleti folyamatokat és az információbiztonsági kontrollokat egyaránt.

Az üzleti célok támogatására készíthető információbiztonsági vízió, illetve maga az információbiztonsági stratégia. A stratégiától befolyásolva a

[11] MSZ ISO/IEC 27001:2014. Informatika. Biztonságtechnika. Az információbiztonság-irányítási rendszerek. Követelmények, Magyar Szabványügyi Testület, 2014.

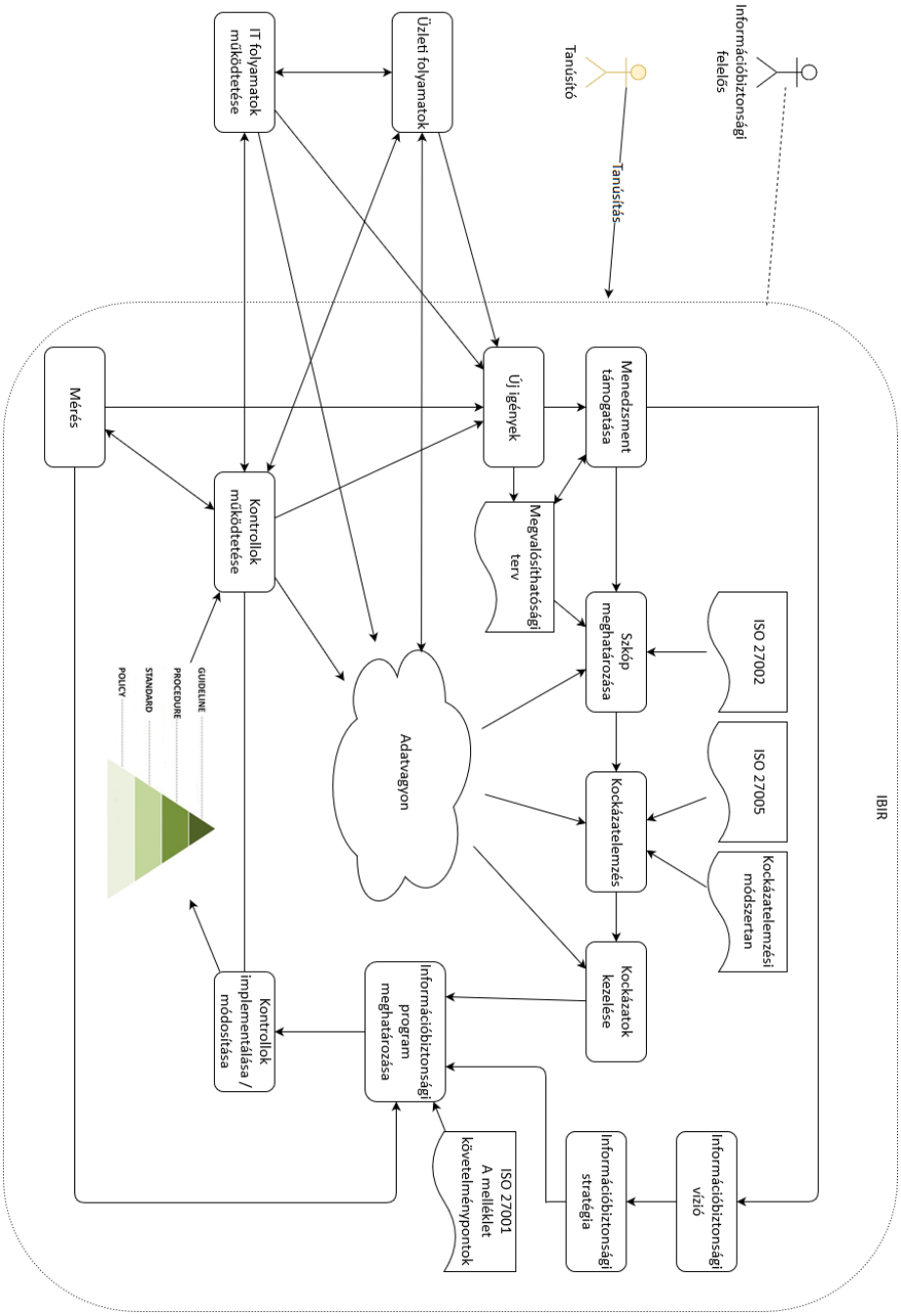
kockázatelemzés során felismert hiányosságok befoltozására készül az aktuális információbiztonsági program.

Az operatív működésbe léptetett adminisztratív, fizikai és logikai kontrollok alapjait az információbiztonsági politika, szabályzat és eljárások adják, melyek maguk is (adminisztratív) kontrolloknak tekintendők. További, meghatározó jellegű támogató folyamat a szabvány A mellékletéből, valamint számos más szabványból (pl. PCI-DSS[12], NIST SP 800-53[13]), illetve jogszabályból (pl. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv. általi felhatalmazás alapján a 41/2015. (VII. 15.) BM rendelet) vagy ajánlásból származhat.

A bevezetett kontrollok működésére vonatkozóan a folyamatos felügyelet vagy épp mintavételezés útján megvalósított visszaméréssel és visszacsatolással biztosítható a folyamatos fejlődés. Az IBIR működését a szabvány ellenében független tanúsító szervezet által tanúsítani lehetséges. A felvázolt egyszerűsített modellt az alábbi ábra szemlélteti:

[12] PCI Security Standards Council: Payment Card Industry (PCI) Data Security Standard, 2016. 04., https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf. (Letöltés ideje: 2018. 03. 20.)

[13] NIST: NIST Special Publication 800-53 Revision 4, 2013. 04., http://dx.doi.org/10.6028/NIST.SP.800. (Letöltés ideje: 2018. 03. 20.)



7. ábra: Az IBIR működésének egyszerűsített modellje
(saját szerkesztés)

Az adatvédelem és az információbiztonság kapcsolódási pontjai

Elemezve az Általános adatvédelmi rendelet jelentette kötelezettségek és az információbiztonság MSZ ISO/IEC 27001:2014 szabvány követelményeinek megvalósítását, a megfelelés kivitelezésében a kapcsolódási pontok jól azonosíthatóak. A korábbiakban többek közt a British Assessment Bureau is elvégezte, mely eredményét 2017. júliusban publikálta[14]. A továbbiakban az általam végzett elemzés eredményét ismertetem.

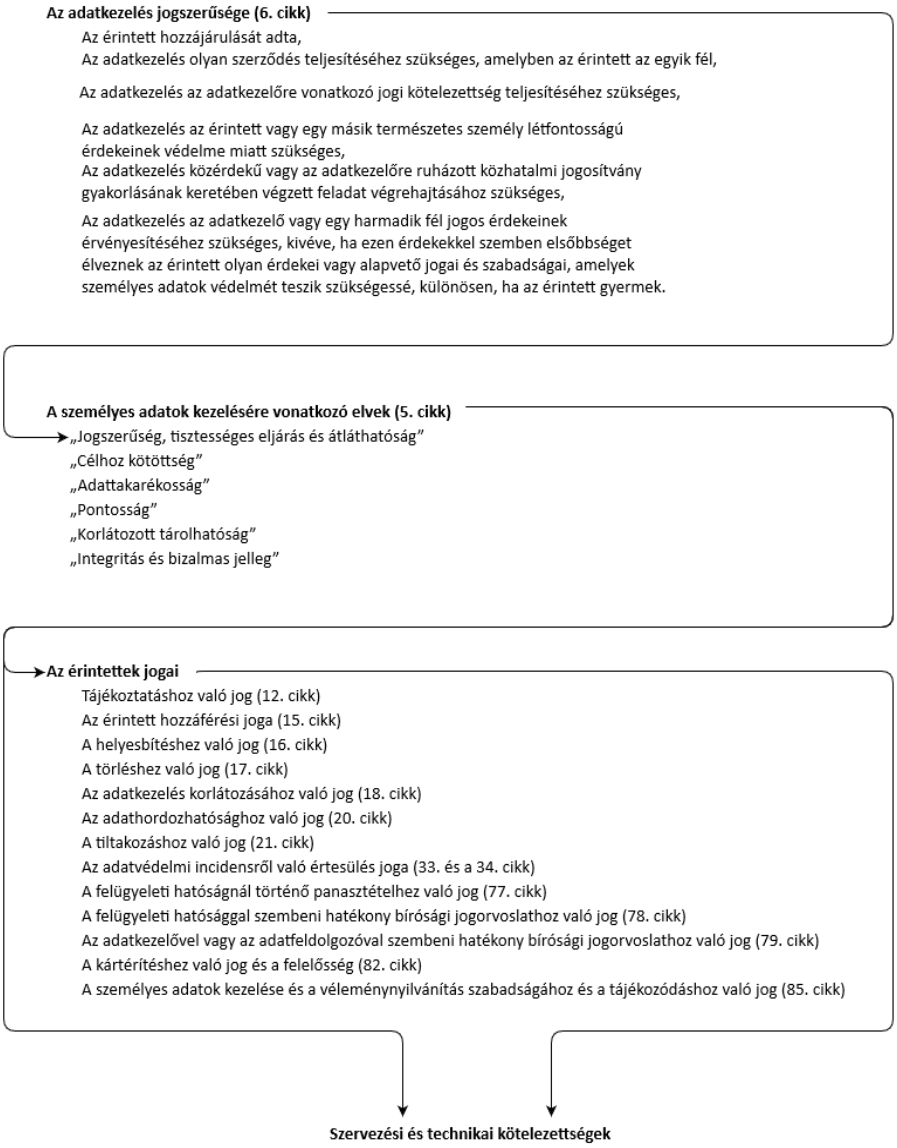
Összességében megállapítható, hogy az Általános adatvédelmi rendelet indukálja az információbiztonság iránti igényt, megköveteli annak tudatos megvalósítását. Az adatkezelési elvek és az érintetti jogok tiszteletben tartása végett megkövetelt kötelező jellegű szervezési és technikai kötelezettségek egyértelműen lefordíthatók az információbiztonság adminisztratív, fizikai és logikai kontrollokká a bizalmasság, a sértetlenség és a rendelkezésre állás biztosítása céljából. Az egyértelműen kötelező jellegű kontrollt az anonimizálás, a titkosítás, a hozzáférés vezérlés jelenti. Továbbá követelményeket fogalmaz meg az incidensmenedzsment és a változásmenedzsment felé. A változások kezelésére vonatkozóan egyértelmű követelmény a „beépített adatvédelem" megvalósítása, továbbá a megfogalmazott feltételek teljesülése esetén a hatásvizsgálat megvalósítása.

Ezen túlmenően utalva (és megismételve) a korábbi megállapításokat az irányítási rendszerekkel kapcsolatos felelősökre vonatkozóan, az ADIR felelőse az Adatvédelmi tisztviselő (vagy a kijelölési kötelezettség hiányában a kijelölt Adatvédelmi felelős), míg az IBIR felelőse az Információbiztonsági felelős.

Az Általános adatvédelmi rendelet alapvetői összefüggéseit szemléltető 8. ábra összefüggéseire alapozva az MSZ ISO/IEC 27001:2014 szabvány A mellékletében szereplő követelmények és az adatkezelési műveletek összefüggéseit a 9. ábra szemlélteti.

Az informatikai rendszerek és szolgáltatások funkcionalitását megkülönböztetve szerepel, mert a helyesbítési és törlési jog teljesítéséhez szükséges módosítási és törlési funkció nem információbiztonsági kontroll. Azonban kiemelkedő jelentőségű, hogy e funkciókhoz a hozzáférés kivitelezéséhez milyen kontrollokat határozunk meg.

[14] The British Assessment Bureau: GDPR & ISO 27001 mapping table, 2017. 07. http://www.british-assessment.co.uk/wp-content/uploads/2017/07/GDPR-ISO-27001-Mapping-Table-2.pdf. (Letöltés ideje:2018. 02. 07.)



8. ábra: Az Általános adatvédelmi rendelet kapcsolata az MSZ ISO/IEC 27001:2014 követelménypontokkal
(saját szerkesztés)

9. ábra: Az Általános adatvédelmi rendelet kapcsolata az MSZ ISO/IEC 27001:2014 követelménypontokkal
(saját szerkesztés)

A személyes adatok és az adatvagyon kapcsolata

Az IBIR keretein belül az információbiztonsági felelős közreműködésével működtetett információbiztonsági kontrollok tárgyát a szervezet teljes adatvagyona jelenti. Az Általános adatvédelmi rendelet az információbiztonság témakörében megfogalmazott adatkezelői, adatfeldolgozói kötelezettségeket a személyes adatokat kezelő információs rendszerek ellenében fogalmazza meg. Ennek értelmében az ADIR tárgya a szervezet valós részhalmazát képező személyes adatok, illetve a személyes adatokat feldolgozó informatikai rendszerek.

Ebből természetesen nem az a következtetés vonható le, hogy csak e rendszereket szükséges megfelelően védeni, minthogy egy támadó minden további nélkül kihasználhatja a másik rendszer sérülékenységét, és átvéve az adott rendszer fölötti irányítást, közvetlen támadást intézhet az adatfeldolgozást végző rendszeren. A fentiek értelmében a személyes adatok az adatvagyon valós részhalmazát képezik.

A hatásvizsgálat és a kockázatelemzés kapcsolata

Az IBIR megköveteli rendszeres időközönként, valamint jelentős beruházást (beszerzést vagy fejlesztést) megelőzően teljes értékű, illetve nagyobb változások esetén a változáskezelési folyamatba integráltan eseti jellegű, fókuszált kockázatelemzés végrehajtását, amelyhez azonosítani szükséges a fenyegetettségeket, sérülékenységeket, valamint az üzleti hatásokat is egyaránt. A felismert kockázatokra az analizálást követően a lehetséges válaszlépéseket szükséges megfogalmazni és a vezetői támogatás mellett ki kell választani a legmegfelelőbb lehetőséget. A kockázatokat ezt követően nyomon kell követni[15].

Az ADIR keretein belül végzett hatásvizsgálatot az Általános adatvédelmi rendelet 35. cikk (1) bekezdés szerint az adatkezelő az adatkezelést megelőzően kell végezni, amennyiben „*különösen új technológiákat alkalmaz* […], *figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve*”. Továbbá a 35. cikk (11) bekezdése szerint „*az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.*”

A 35. cikk (7) bekezdése szerint a hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére,
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára,
- az érintettek jogait és szabadságát érintő kockázatok vizsgálatára,
- a kockázatkezelést célzó intézkedések bemutatására (beleértve a személyes adatok védelmét és a rendelet által megfogalmazott kötelezettségek teljesítésének bizonyítására szolgáló, az érintettek és más személyek jogait

[15] ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management, International Organization for Standardization, 2011.

és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat).

A változások során elvégzendő kockázatelemzés és hatásvizsgálat kezdeményezésében a változásmenedzsmentnek nagy szerepe van.

Az adatvédelmi nyilvántartás és az adatvagyon nyilvántartás kapcsolata

Az IBIR működtetésének egyik alapja az információbiztonsági attribútumokat tartalmazó adatvagyon-nyilvántartás létrehozása és annak karbantartása. A nyilvántartás tartalma az azonosított elemi adat vagy adatkör, a lokalizáció, az adatgazda és további szerepkörök (felhasználók, adminisztrátorok stb.), valamint bizalmasság, sértetlenség és rendelkezésre állás szerinti osztályozás (és elemzés).

Az adatvédelmi nyilvántartás (adatkezelési tevékenységek nyilvántartása) a 30. cikk (5) bekezdése alapján az alábbi esetekben kötelező jellegű:

- legalább 250 fő személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha:
  - az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár,
  - az adatkezelés nem alkalmi jellegű,
  - az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

A 30. cikk (1) bekezdése szerint minden adatkezelő az által végzett adatkezelési tevékenységekről nyilvántartást vezet, melynek kötelezően tartalmaznia kell az alábbiakat:

„- az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;

- *az adatkezelés céljai;*
- *az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;*
- *olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;*
- *adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;*
- *amennyiben lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;*
- *amennyiben lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.”*

A 30. cikk (2) bekezdése szerint minden adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról, melynek kötelezően tartalmaznia kell az alábbiakat:

„- az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;

- *az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;*
- *adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;*
- *ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása."*

A tartalmi elemekben hivatkozott, ezt megelőzően nem tárgyalt 49. cikk a személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítását szabályozza.

Mindkét nyilvántartás karbantartásában a rendszeres felülvizsgálatnak, illetve a változások során elvégzendő frissítési művelet kezdeményezésében a változásmenedzsmentnek nagy szerepe van.

Az adatvédelmi incidens és az információbiztonsági incidens kapcsolata

Az MSZ ISO/IEC 27002:2011 alapján az információbiztonsági incidens *„egyetlen vagy egy sorozat nem kívánt vagy nem várt olyan információbiztonsági esemény, amely bekövetkezésének jelentős az üzleti műveleteket veszélyeztető és az információbiztonságot fenyegető valószínűsége van"*[16].

Ezzel szemben az adatvédelmi incidens a 4. cikk 12. szerint „*a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi*."

Az adatvagyon és a személyes adatok viszonyához hasonlatosan az adatvédelmi incidensek az információbiztonsági incidensek valós részhalmazát képezik. Ennek következtében az adatvédelmi incidensek kezelése integrálható az IBIR szerinti incidenskezelési folyamatba.

A beépített és alapértelmezett adatvédelem és a beépített védelem kapcsolata

Az információbiztonság egyik meghatározó alapelve a beépített és integrált védelem (Privacy by design and by default), amely szerint a biztonsági

[16] MSZ ISO/IEC 27002:2011 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve, 2011, p. 26.

követelményeket és azok alapján az információbiztonsági követelményeket a beszerzési és fejlesztési projektek elején specifikálni szükséges, valamint a projektfeladatok végrehajtása során fokozatosan és értelemszerűen az adott folyamat és a rendszer részévé kell tenni. A beépített és alapértelmezett adatvédelem (Security by design) annyiban egészíti ki az előbbi elvet, hogy a folyamat során kezelt személyes adatok körét, a kezelés körülményeit az Általános adatvédelmi rendeletben meghatározott, a korábbiakban tárgyalt elvek és jogok szerint kell megtervezni és végrehajtani.

Az együttműködés szükségessége

Általánosan elmondható, hogy a mindenkori jogszabályi követelményeknek való megfelelés jelentős ráfordítást igényel a szervezetektől. Ez az információbiztonság területére kifejezetten érvényes megállapítás.

Ezt a tényt, továbbá a kockázatkezelés (mondhatni) mindent átszövő jelenlétét felismerve került formalizálásra az irányítás, kockázatkezelés és megfelelés hármasa (Governance, Risk management, Compliance – GRC). Az OCEG (Open Compliance and Ethics Group)[17] definíció szerint a GRC „*olyan képességek, szemléletmód, valamint tevékenységek gyűjteménye és együttese, amellyel a működés során felmerülő bizonytalanság és komplexitás a szervezeti funkciók irányításában kezelésre kerül*”[18]. A GRC tehát a működéshez szükséges tevékenységek olyan szervezési módja, amely elősegíti annak hatékony megvalósítását, az ahhoz szükséges struktúra és folyamatok kialakítását.

A GRC folyamatok a szervezet egészét érintik, amely által definiált módon a vállalati, szervezeti vérkeringésbe kapcsolódik az informatika, az információ- (ez által az informatikai) és a fizikai biztonság egyaránt. A kapcsolódó folyamatok az elvárásoknak megfelelő működési helyességét a megfelelés kérdésköre kezeli, mely a vezetői szinten meghatározott célok elérése érdekében létrehozott stratégia, valamint az aktuális jogi és iparági előírások figyelembe vételével megalkotott szabályrendszerhez való alkalmazkodás, annak megfelelő működés, továbbá az attól való eltérés (kivételek) kezelése.

Összefoglalás

Az információbiztonság a történelem során az emberi tevékenység részét képezte, melyre kiváló példát nyújt a Caesar-kód és a Vigenère titkosító évezredekkel, illetve évszázadokkal ezelőtti alkalmazása[19]. A titkosítással együtt az információbiztonsági kontrollokon relatíve lassú fejlődés, illetve megújulási folyamat érvényesült. Ehhez képest a közelmúltban az informatikai eszközök, informatikai rendszerek megjelenése és széleskörű elterjedése forradalmasította az információfeldolgozást, amelybe szép lassan az információbiztonsági követelmények is integrálódtak. E változás, azaz a technikai fejlődés, a gazdasági, társadalmi változások magával hozták a személyes adatok minél szélesebb rögzítését

[17] https://www.oceg.org/
[18] OCEG: What is GRC?, http://www.oceg.org/what-is-grc/. (Letöltés ideje: 2017. 05. 21.)
[19] VIRASZTÓ Tamás, Titkosítás és adatrejtés, NetAcademia Kft., 2004.

és feldolgozását. E folyamat közben az információ és ezzel a személyes adatok értéke mindinkább felértékelődött, megteremtve az információs társadalmat.

A személyes adatok vonatkozásában az informatikai (számítógépes) adatfeldolgozás szabályozását a magyar jogrendszer már 1981-ben megvalósította az 1/1981. (I. 27.) BM rendelettel. A személyes adatok általános jellegű szabályozását a 15/1991 (IV. 13.) AB-határozat következtében a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) szabályozta. Magyarország Európai Unióhoz történő csatlakozását követően az uniós jog alkalmazása megkerülhetetlenné vált. A 2011. évi CXII. törvény meglehetős késedelemmel ültette át az 1995-ös Európai Parlament és a Tanács 95/46/EK irányelvet a magyar jogrendszerbe. Az Európai Parlament és a Tanács 2016/679 rendelet (Általános adatvédelmi rendelet) közvetlen hatályából eredően, annak alkalmazása 2018. május 25-től elkerülhetetlen.

Az információbiztonsági és az adatvédelmi követelmények figyelembevétele és kötelezettségek teljesítése manapság is jelentős hiányosságokat mutat. Az adott szervezet képességeinek megfelelő szintű információbiztonság és adatvédelem bevezetése, ezek fenntartása, folyamatos fejlesztése megfelelő szervezet, tudás, felsővezetői támogatás, attitűd stb. mellett egy-egy irányítási rendszer működtetésével valósítható meg.

A két elkülönülő irányítási rendszer bevezetése, együttműködésük, de még inkább integrált működésük elősegítése kulcsfontosságú, hiszen az Általános adatvédelmi rendeletben foglalt, valamint az azt követően hatályos Infotv. és a különböző ágazati törvények jelentette kötelezettségekre 2018. május 25-ig a vállalatokat, szervezeteket fel kell készíteni. Azonban a május 25-i mérföldkőtől számítva a megfelelést folyamatosan biztosítani kell. Úgy gondolom, hogy az adatvédelem ilyen jellegű (valóban általános) szabályozása az információbiztonságra is nagy hatással lehet, meghozva a kívánt áttörést, hogy a közszféra és a versenyszféra egyaránt megfelelő komolysággal kezelje mindkét kérdéskört.

Felhasznált irodalom:

- Bureau Veritas: Technical Standard related to personal data protection in compliance with the regulation (EU) 2016/679, 2017. http://www.bureauveritas.hu/4856710d-67db-4b65-918b-7ac912b335d1/Data+Protection_Technical+standard_Bureau+Veritas.pdf?MOD=AJPERES. (Letöltés ideje: 2018. 02. 15.)
- ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management, International Organization for Standardization, 2011. http://www.iso27001security.com/html/27005.html
- MSZ ISO/IEC 27002:2011 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve, 2011, p. 26.

- MSZ ISO/IEC 27001:2014. Informatika. Biztonságtechnika. Az információbiztonság-irányítási rendszerek. Követelmények, Magyar Szabványügyi Testület, 2014.
- NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2013. évi tevékenységéről, 2014. http://naih.hu/files/NAIH-beszamolo2013--MID-RES.pdf. (Letöltés ideje: 2018. 01. 20.)
- NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2012. évi tevékenységéről, 2013. http://naih.hu/files/NAIH_BESZaMOLo_2012_net3.pdf. (Letöltés ideje: 2018. 01. 20.)
- NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2014. évi tevékenységéről, 2015. http://naih.hu/files/NAIH-2014-eves-beszamolo-magyar-MR.pdf. (Letöltés ideje: 2018. 01. 20.)
- NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2015. évi tevékenységéről, 2016. http://naih.hu/files/NAIH-BESZ-MOL--2015-MID-RES.pdf. (Letöltés ideje: 2018. 01. 20.)
- NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2016. évi tevékenységéről, 2017. http://naih.hu/files/NAIH-BESZ-MOL--2016_Mid-Res.pdf. (Letöltés ideje: 2018. 01. 20.)
- NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2017. évi tevékenységéről, 2018. http://naih.hu/files/NAIH-BESZAMOLO-2017-mid-res.pdf. (Letöltés ideje: 2018. 04. 24.)
- NIST: NIST Special Publication 800-53 Revision 4, 2013. 04. http://dx.doi.org/10.6028/NIST.SP.800. (Letöltés ideje: 2018. 03. 20.)
- OCEG: What is GRC?, http://www.oceg.org/what-is-grc/ (Letöltés ideje: 2017. 05. 21.)
- PCI Security Standards Council: Payment Card Industry (PCI) Data Security Standard, 2016. 04. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf. (Letöltés ideje: 2018. 03. 20.)
- Ponemon Institute LLC: The Need for a New IT Security Architecture: Global Study on the Risk of Outdated Technologies, 2017. 02. https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/ponemon-institute-security-study-outdated-technology-risks.pdf. (Letöltés ideje: 2018. 03. 21.)
- Ponemon Institute LLC: The Need for a New IT Security Architecture: Global Study, 2017. 01. https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/ponemon-security-study.pdf. (Letöltés ideje: 2018. 03. 21.)
- Ponemon Institute LLC: 2017 Cost of Data Breach Study, 2017. 06. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN. (Letöltés ideje: 2018. 01. 15.)

- The British Assessment Bureau: GDPR & ISO 27001 mapping table, 2017. 07. http://www.british-assessment.co.uk/wp-content/uploads/2017/07/GDPR-ISO-27001-Mapping-Table-2.pdf (Letöltés ideje: 2018. 02. 07.)
- Trend Micro Inc.: Russian Underground 101, 2012. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf. (Letöltés ideje: 2018. 01. 14.)
- VIRASZTÓ Tamás: Titkosítás és adatrejtés, NetAcademia Kft., 2004.

Felhasznált jogszabályok:

- 1/1981. (I. 27.) BM rendelet
- 15/1991 (IV. 13.) AB-határozat – információs önrendelkezési jog
- 1992. évi LXIII. törvény
- Code of Federal Regulations 200.79 §
- 2011. évi CXII. tv. (Infotv.)
- 2013. évi L. törvény
- 41/2015. (VII. 15.) BM rendelet
- Európai Parlament és a Tanács 2016/679 rendelete
- Európai Parlament és a Tanács 95/46/EK irányelve

FEKETE CSANÁD

HADVISELÉS AZ INFORMÁCIÓS KORSZAKBAN AZ ÚJ PARADIGMA KÜSZÖBÉN?[1]

Bevezetés

A hidegháború lezárulása nemcsak politikai és hatalmi átrendeződést vont maga után; számos olyan társadalmi és technológiai folyamat zajlott ebben az időszakban, melyek hatására átalakult a globális biztonsági környezet. Ezek közül kiemelhető az infokommunikációs technológiák (a továbbiakban: IKT) robbanásszerű fejlődése és széleskörű elterjedése, mely megnyitotta egy új virtuális környezet, a kibertér kapuját. Ezzel kezdetét vette az emberi történelem talán legjelentősebb társadalmi és gazdasági változása, mely a biztonság valamennyi területére hatással volt. Az új információs korszakban sohasem látott módon kapcsolódtak össze a biztonságot érintő szektorok, a korábban leküzdhetetlen földrajzi határok röviddel a vasfüggöny ledőlését követően bizonyos értelemben feloldódtak az új virtuális térben. Az új nemzetközi környezetben a globalizáció és a hatalmi viszonyok átrendeződése is kezdte egyre inkább elmosni a béke és háború, a harcolók és nem harcolók, valamint a hadszíntér és hátország közötti határvonalakat. A lokális és regionális konfliktusok egyre komplexebbé váltak, hatásaik pedig a legtöbb esetben átnyúlnak az adott régió határain. A technológiai fejlődés és társadalmi jelenségek vizsgálata az új hadelméleti irányzatok központi témájává vált, melyek mind az államszint alatti szereplők felemelkedéséből, mind a hadviselés átalakulásából indultak ki. Egyes szerzők ezek alapján paradigmaváltásról és egy új hadügyi forradalom kibontakozásáról kezdtek beszélni, melynek motorját az információs technológiák robbanásszerű fejlődésében vélték felfedezni.

Ennek értelmében először célszerű megvizsgálni az információs forradalom hadviselésre gyakorolt hatásait, amit álláspontom szerint érdemes három, kronológiailag egymást követő részre osztani:

1. a hadügyi forradalomra és a konvencionális hadviselés átalakulására;
2. az információs tér létrejöttére és a stratégiai hadviselés változásaira;
3. a stratégia 21. századi átalakulására.[2]

A három témakör részletes bemutatása meghaladja ezen írásmű kereteit, ezért az információs tér szerepének vizsgálatára helyezem a fő hangsúlyt. A kutatás legfőbb kiindulópontja, hogy a közelmúltban – a technológiai fejlődés, valamint az IKT horizontális terjedése révén stratégiai jelentőségűvé váltak az információs környezetben folyó műveletek, ami fokozatosan átformálja a konfliktusok természetét az alkalmazott stratégiák, eszközök, valamint módszerek

[1] A publikáció az Emberi Erőforrások Minisztériuma ÚNKP 17-3-I-NKE-58 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

[2] Bővebben lásd: FEKETE Csanád: Információ és hadviselés – háború a kognitív hadszíntéren I., Szakmai Szemle, 2016, XIV. évf. 3. sz. pp. 24-41.

vonatkozásában. Ennek tükrében jelen írásban az alábbi kérdésekre keresem a választ:

- Tényleg beszélhetünk egy hadügyi paradigmaváltásról, és ha igen, melyek ennek főbb jellemzői?
- Az elmúlt évek eseményeit tekintve beszélhetünk-e a stratégiai információs hadviselés megjelenéséről?
- Amennyiben a válasz igen, a stratégiai információs hadviselésnek milyen főbb jellemző jegyei vannak és milyen célokra lehet alkalmazni?

Ezek megválaszolásához első lépésként – a vonatkozó szakirodalom és az utóbbi két évtized tapasztalatai alapján – olyan általános megállapításokat tettem, melyek a kutatás legfőbb iránymutatójaként szolgálnak, és várakozásaim szerint igazolást fognak nyerni a publikáció végén:

a) A konvencionális hadviselés tekintetében:

– az információs forradalom gyökeres változásokat idézett elő a konvencionális hadviselés terén, melynek hatására előtérbe kerültek az információalapú tevékenységek és létrejött a hálózatközpontú hadviselés koncepciója;[3]

– az információs korszakban a fizikai pusztítás helyett a hangsúly egyre inkább a szemben álló fél vezetési és irányítási rendszerének bénítására, valamint az ellenséges erők harcképességének megtörésére helyeződött át, ezzel párhuzamosan előtérbe került a katonai műveletek hatásalapú megközelítése;

– e folyamatot az infokommunikációs technológiák rohamos fejlődése, a nagy pontosságú fegyverrendszerek, valamint a vezetési, irányítási, kommunikációs, informatikai, felderítő, hírszerző, megfigyelő és felderítő rendszerek (Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance – C4ISR) kifejlesztése és tömeges hadrendbe állítása tette lehetővé;

– a folyamat közel sem ért véget, a változások a jövőben várhatóan át fogják alakítani a fegyveres erők felépítését és eszközrendszerét, a hadügyi forradalom jövőbeni szakaszában pedig egyre nagyobb hangsúly fog kerülni a robotika és a mesterséges intelligencia katonai alkalmazására.[4]

---

[3] A nagy mennyiségű, megbízható és pontos információ megszerzése és felhasználása természetesen a korábbi évszázadokban is a hadviselés fontos részét képezte, azonban az új katonai informatikai rendszerek megjelenésével és fejlődésével ezen a területen jelentős változások következtek be, melyek hatására kialakult az úgynevezett digitális harctér és lehetővé vált a harcmező vizualizálása. A hálózatközpontú hadviselés lényegét egy egységes és összekapcsolt számítógépes hálózat adja, ami összeköti a harctéri szenzorokat, a végrehajtó elemeket, valamint a döntéshozókat, közel valósidejű kommunikációt téve lehetővé. Mindez kevesebb erő bevetésével teszi lehetővé a kitűzött célok teljesítését, javítja a reagálóképességet és jelentős mértékben növeli hatékonyságot. Bővebben lásd: HAIG Zsolt – VÁRHEGYI István: Hadviselés az információs hadszíntéren, Budapest, Zrínyi Kiadó, 2005. p. 158-174.

[4] A jövőbeni trendekről jó áttekintést nyújt a Chuck Hagel volt amerikai védelmi miniszter által 2014-ben meghirdetett harmadik offset stratégia. Lásd még: PORKOLÁB Imre:

b) A stratégiai hadviselés tekintetében:

- a kibertér megjelenésével és az IKT eszközök széleskörű térnyerésével megjelent az információs hadviselés koncepciója,[5] majd létrejött a katonai műveletek legújabb információs tartománya;[6]
- a konfliktusok információs tartománya az utóbbi években stratégiai jelentőségre tett szert, mivel a célország információs rendszerei ellen indított összehangolt támadásokkal a létfontosságú rendszerek és létesítmények működése időlegesen megzavarható vagy tartósan megbénítható, ami stratégiai jelentőségű politikai, társadalmi és gazdasági hatásokat idézhet elő;
- az információs hadviselés koncepciója eltérő fejlődési utat járt be nyugaton és keleten, a célok, eszközök és módszerek tekintetében is számos különbséget figyelhetünk meg;
- a fegyveres konfliktusok alatt zajló információs műveletek mellett megjelent az úgynevezett információs konfrontáció, melyben az információ fegyverként kerül alkalmazásra és megszakítás nélkül egyaránt folyhat béke és háborús időszakban;
- az információs konfrontáció szerves részét képező komplex befolyásolási műveletek[7] elsősorban a kognitív tartományban fejtik ki hatásukat, céljuk pedig a célország ellenállóképességének és stratégiai pozíciójának gyengítése, a döntéshozatali rendszer megbénításán és a társadalmi rend aláásásán keresztül.

Innováció – a jövő hadviselésének meghatározó eleme a változókörnyezetbe, Felderítő Szemle, 2015, 14. évf. 3. sz. 2015. pp. 166-175.; ÁRPÁD Zoltán: Intelligens biztonság, hétköznapi problémák – intelligens megoldások, Szakmai Szemle, 2018, XVI. évf. 1. sz. pp. 33-56.

5 Az információs hadviselés első definícióját Thomas P. Rona, az Egyesült Államok védelmi minisztériumának magyar származású kutatója alkotta meg 1976-ban. Rona definíciójában az információs eszközök és módszerek béke- és háborús időszakban történő koordinált alkalmazásáról ír, melyek stratégiai, hadműveleti és harcászati szinten egyaránt folyhatnak, segítve a kitűzött célok elérését. A nyugati országokban a terminológia mára megváltozott és az információs hadviselés fogalma helyett később az információs műveletek megjelölés vált hivatalossá. Bővebben lásd: HAIG Zsolt: Az információs hadviselés kialakulása, katonai értelmezése, Hadtudomány, 21.évf. 1-2. sz. 2011 p. 12

6 A katonai műveletek működési tartománya az utóbbi években túllépett a földrajzi kereteken, az információs térben folyó műveletek legfőbb célja az információs fölény és uralom elérése, melyek kevesebb erőforrás bevonásával és a veszteségek csökkentésével teszik lehetővé a győzelem kivívását. HAIG Zsolt – VÁRHEGYI István: A cybertér és a cyberhadviselés értelmezése, Hadtudomány, 18. évf. E. sz. 2008. p. 2.

7 A befolyásolási műveletek általában a célország történeti, nyelvi, kulturális és társadalmi viszonyaihoz igazodnak, és a kijelölt stratégiai célokkal összhangban a percepciók megváltoztatása, az alternatív valóságok megteremtése, a közvélemény összezavarása, valamint a politikai döntéshozatal befolyásolása céljából folynak. FEKETE Csanád: Információ és hadviselés háború a kognitív hadszíntéren II., Szakmai Szemle, 2016, XIV. évf. 4. sz. p. 51.

c) A stratégia 21. századi átalakulása tekintetében:

– az információs korszakban a stratégia diszciplínája is új irányokba fejlődött, felértékelődtek az indirekt eszközök, melyek segítségével kinetikus műveletek végrehajtása nélkül is lehetővé vált az akarat kikényszerítése és a stratégiai hatások kiváltása.

Az indirekt eszközök térnyerése

A téma szempontjából érdemes egy kis elméleti kitekintést tenni, mellyel célom, hogy az államok között folyó hatalmi harcban, és az akarat másik félre történő rákényszerítése tekintetében vizsgáljam meg a hadviselésben bekövetkezett változások jelentőségét. Jelen írásban Carl von Clausewitz híres tételéből indulok ki, mely szerint a háború nem más mint: „*az erőszak* alkalmazása, aminek célja, hogy az *ellenfelet* saját *akaratunk* teljesítésére *kényszerítsük."*[8] Clausewitz az erőszakon elsődlegesen a fizikai erő alkalmazását értette – melynek a letéteményese a haderő –, ami egy eszköz a politika kezében, hogy elérje kitűzött céljait.

A háborúban alkalmazható eszközök kapcsán viszont leszögezi, annak végeredményében csak egy formája létezik: a harc – ami sokrétű lehet: „*minden, ami a háborúban történik, a haderő által történik."*[9] Ilyen értelemben a háborús célok elérése csakis a haderő alkalmazásán keresztül, fizikai erőszak által és az ütközetek útján történhet. Clausewitz felfogásában a háború végkimenetelét lényegében az ütközetek és a bennük folyó harc határozza meg, melyek a tulajdonképpeni háborús tevékenység alapját jelentik és minden más ezeknek van alárendelve.[10] Clausewitz elméletében az ütközet a fizikai és erkölcsi – morális – erők véres és pusztító összemérése, az a fél győz, akinek több marad a harc végén. Ezzel kapcsolatban leszögezi, hogy az erkölcsi és a fizikai erőveszteség között szoros összefüggés áll fenn, egymást erősítő tényezőknek tekinthetők, melyek meghatározzák a háború végkimenetét.[11]

A szemben álló haderő megsemmisítése tehát egy eszköz az ütközet céljának – a győzelem kivívásának – eléréséhez, melynek értelmében a háborús tevékenység alapja az ellenség megsemmisítése. A háborús tevékenység végső célja pedig az ellenség védekezésre képtelenné tétele a hadereje lefegyverzése vagy legyőzése, akarata megtörése és területe birtokbavétele révén.[12]

A háború logikája szerint e tevékenységeknek az alábbi sorrendben kell történnie: elsőként az ellenséges erőket kell megsemmisíteni, hogy a másik fél ne tudja tovább folytatni a harcot, ezt követően a területét meg kell szállni, hogy ne tudjon új haderőt szervezni, majd akaratát meg kell törni, hogy a harcok ne lángoljanak újból, végül a kormányzatát rá kell kényszeríteni a béke aláírására, a lakosságát pedig be kell hódoltatni.[13] A háború voltaképp az államok közötti

---

8 CLAUSEWITZ, Carl von: A háborúról, Zrínyi Kiadó, Bp., 2014, p. 37.
9 Uo., p. 64.
10 Uo. p. 230.
11 Uo. p. 238.
12 Uo. pp. 40-41.
13 Uo. pp. 57-65.

érdekek konfliktusa, melyek megoldása erőszakos formában, vérrel történik, és ez különbözteti meg a háborút a többi konfliktustól.

E definíciók alapján több megállapítást is tehetünk: az államok céljaikat elsősorban erőszakos eszközökkel kívánják elérni, a legfőbb eszköz Clausewitz korában a haderő volt, így az államok elsősorban fegyveres úton, a fizikai erő alkalmazásával kényszerítették rá akaratukat a másik félre. Ebben az értelemben viszont a háború maga is egy eszköz a politika kezében, amit az érdekei védelmében, az akarata kikényszerítésére használ. Amennyiben ezt a kijelentést elfogadjuk, és számba vesszük az elmúlt évszázad változásait, valamint technológiai fejlődését, akkor beláthatjuk, hogy Clausewitz korához képest jelentősen kibővült az államok rendelkezésére álló eszköztár. Az államok ugyanis a haderő mellett napjainkban számtalan más – erőszakos – eszközzel tudnak érvényt szerezni akaratuknak. Ugyanakkor továbbra is igaz, hogy a haderő és a háború érdekérvényesítése az eszköztár meghatározó része maradt, vagyis a konfliktusok feloldására szolgáló „végső érv."

A korábbi évszázadokban – sőt még a XX. század közepén is – a katonai erő volt az államok legfőbb kényszerítő eszköze, így a biztonsággal és a stratégiával foglalkozó kutatások túlnyomó részt a háborúkra, valamint a katonai-fegyveres dimenzióra fókuszáltak. Napjainkban azonban olyan új – pontosabban inkább megújult – eszközök jelentek meg és váltak az állami erőszak-eszköztár részévé, melyek révén megtörhető a szemben álló fél akarata és akár fizikai harc nélkül is elérhetők a kitűzött célok. Ezzel kapcsolatban érdemes két fogalmat megkülönböztetni egymástól: az ellenség megsemmisítése céljából folyó direkt és annak kifárasztása érdekében folytatott indirekt hadviselést.[14] Ebből is látszik, hogy az előbbi az erők közvetlen összemérésén, míg az utóbbi a küzdelem elnyújtásán és a döntő csata elkerülésén alapszik. Az egyik harcban akarja legyőzni a másik oldalt, míg a másik morálisan és erkölcsileg akarja kifárasztani és megtörni az ellenséget. E nézőpontból a katonai erő az államok direkt, míg a diplomáciai, információs vagy gazdasági erő indirekt eszközöknek számítanak.

Clausewitz elsősorban a hadviselés direkt formájával foglalkozott, az indirekt megközelítés jobb megértéséhez érdemes röviden bemutatni az ókori Kína egyik legjelentősebb katonai teoretikusa, Szun-ce néhány gondolatát. A szerző *„Háború művészete"* című könyvében foglalta össze gondolatait, az általa leírt elvek jelentős hatást gyakoroltak a hadviselés fejlődésére, melyben többek között az alábbi megállapítások találhatók a háború vonatkozásában:
„A háború mindig a csalás útját járja. Így ha képesek vagyunk valamire, tegyünk úgy, mintha nem lennénk rá képesek; ha valamit felhasználunk, tegyünk úgy, mintha nem használnánk fel; ha közel vagyunk, keltsük azt a látszatot, hogy távol vagyunk; ha távol vagyunk, keltsük azt a látszatot, hogy közel vagyunk; előnyöket kínálva csalogassuk (az ellenséget), sorait megzavarva mérjünk csapást reá; ha mindene megvan, jól készüljünk fel ellene; ha erősebb nálunk, kerüljük el (az összecsapást); ha dühös, vezessük félre; magunkat alantasabbnak mondva tegyük elbizakodottá; ha friss erővel rendelkezik, fárasszuk ki; ha (egységei) szoros kapcsolatban vannak, ziláljuk szét őket; ott támadjuk meg, ahol nem készült fel a védekezésre, s akkor küldjük előre (csapatainkat), amikor (az ellenség) éppenséggel nem várja."[15]

---

[14] CLAUSEWITZ i.m. p. 31.

[15] SZUN-CE: A hadviselés törvényei, Budapest, Balassi Kiadó, 1998, p. 4.

E rövid idézetből is látható, hogy a kínai szerző a győzelem elérésének kulcsfontosságú eszközeiként tekintett az olyan indirekt módszerekre, mint a meglepés, a manőverek, a megtévesztés, vagy a terep sajátosságainak kihasználása. A hadviselés alapvető törvényszerűsége kapcsán pedig többek között az alábbi útmutató olvasható művében:
„Így aki igazán ért a hadviseléshez, úgy töri meg az idegen sereget, hogy nem vív csatát vele; úgy foglalja el az idegen városfalat, hogy nem ostromolja meg; úgy semmisíti meg az idegen fejedelemségeket, hogy nem tart sokáig (a háború). S minthogy a (kölcsönös) sértetlenség által igyekszik győzni az égalattiban, a fegyverek alkalmazása nélkül is biztosítani tudja magának az előnyöket. Ez a csellel való támadás törvénye."[16]

A téma szempontjából különösen fontos tanulsággal szolgálnak a második idézetben található gondolatok, melyek rávilágítanak arra a tényre, hogy az indirekt hadviselés alapvető elvei és céljai mit sem változtak az évezredek során, az új jelenségek csupán az eszközök és módszerek változásaiban keresendők. Az elmúlt évtizedek stratégiai jelentőségű[17] fejleményei közül elsősorban az információs technológiák robbanásszerű fejlődése és a kibertér megjelenése emelhető ki, ami forradalmi változást hozott magával, lehetővé téve az államok – és államszint alatti szereplők – számára, hogy direkt katonai eszközök alkalmazása nélkül kényszerítsék rá akaratukat a másik félre.

A stratégia indirekt megközelítése szempontjából Basil Henry Liddell Hart munkássága megkerülhetetlennek számít, aki az első világháborút követően maradandót alkotott az indirekt stratégia és a nagystratégia módszertanának kidolgozásával. Az első világháború tapasztalataiból kiindulva arra a következtetésre jutott, hogy a szemben álló erők fizikai megsemmisítését célzó közvetlen (*direkt*) megközelítés szinte sohasem kifizetődő. Ehelyett célszerű az úgynevezett indirekt megközelítést alkalmazni,[18] melyben a fő erőfeszítések az ellenség eredeti szándékától való eltérítésére irányulnak, a kezdeményezés megragadása, a szemben álló fél egyensúlyi helyzetének megtörése, vezetésének megtévesztése, csapatai harcképességének és moráljának aláásása által. Ennek értelmében Liddell Hart szerint a sikeres stratégia – Szun-ce elveihez hasonlóan – a meglepésre, a manőverre, a bekerítésre és a megtévesztésre épül.

Ezt követően a szerző 1967-es könyvében a stratégia indirekt megközelítésének általa már korábban megfogalmazott elméletét tovább bővítette, megalkotva a „nagystratégia" koncepcióját, melyről művében az alábbiakat írja:

---

16 SZUN-CE i.m. p. 6.

17 Ezt megelőzően a nukleáris fegyverek és az interkontinentális ballisztikus rakéták megjelenése okozott hasonló stratégiai jelentőségű változásoka a hadviselésben.

18 Liddel Hart a sikeres stratégia és taktika kapcsán 6 pozitív (1. célok és eszközök összehangolása, 2. célok szem előtt tartása, 3. váratlan és a 4. legkisebb ellenállás irányába történő támadás, 5. alternatív célpontokat kínáló támadási irány választása, 6. rugalmas harcrend és műveleti terv kidolgozása) és 2 negatív (1. nem szabad a főerőket bevetni, ha a szemben álló fél megtette a szükséges előkészületeket és megfelelően felkészült, 2. kudarc esetén nem szabad ugyanabban az irányban és ugyanazzal a módszerrel támadni) maximát fogalmazott meg. LIDDELL HART, Basil Henry: Stratégia, Budapest, Európa Könyvkiadó, 2002. p. 515.

„A nagystratégia – magasabb stratégia – szerepe ugyanis az, hogy koordinálja és irányítsa a nemzet vagy az országcsoport minden erőforrását a háború politikai célkitűzéseinek elérésére, amelyeket viszont az alapvető politika fogalmaz meg... Mi több, a harcoló erő csupán egyik eszköze a nagystratégiának, mert ez utóbbi számításba veszi és alkalmazza a pénzügyi, a diplomáciai, a kereskedelmi és, nem utolsósorban, az etikai nyomás eszközeit is az ellenfél akaratának gyengítése érdekében. A jó ügy kard is, páncél is. Ugyanígy, a lovagiasság a háborúban roppant hatékony fegyver lehet az ellenség ellenálló képességének meggyengítésében és a saját morális erők fokozásában."[19]

A nagystratégia koncepciója nagy hatást gyakorolt a stratégiai gondolkodásra, melynek köszönhetően a hidegháború éveiben egyre jelentősebbé váltak az indirekt – nem-katonai – eszközök, mivel a nukleáris fegyverek által kölcsönösen biztosított megsemmisítés árnyékában egy direkt katonai konfrontáció végzetes következményekkel járt volna a világra nézve. Ezen túl a korszak töretlen technológiai fejlődése lehetővé tette, hogy az stratégia eszköztára tovább bővüljön, így nem meglepő, hogy a bipoláris világrend megszűnését követően az indirekt megközelítés még fontosabbá vált.

Végül fontos még megemlíteni John Boyd-ot és az általa kidolgozott döntési ciklus elméletét (Observe, Orient, Decision, Act – OODA loop – Megfigyelés, Orientáció, Döntés, Cselekvés ciklusa), ami az információs hadviselés koncepciója szempontjából is kiemelkedő fontossággal bír. Az OODA ciklus első két lépésében a döntéshozó célja az események és folyamatok észlelése, valamint a környező világól alkotott modelljének felülvizsgálata és frissítése.[20] Ezt követően döntés születik a jövőbeni intézkedésekről, majd végső lépésként megtörténik azok végrehajtása. A meghozott intézkedések változásokat idéznek elő a környezetben, melynek hatására felülvizsgálatra szorul a világról alkotott modell és a döntéshozatali ciklus újraindul.

Boyd elméletének lényege egy olyan stratégiai tervezési módszerben rejlik, ami az OODA ciklus gyorsabb végrehajtása által lehetővé teszi a kezdeményezés megragadását és a vezetési fölény kivívását.[21] A koncepcióban nagy szerep jut a másik fél vezetési és döntési ciklusának megzavarására, nagyban épít a

---

19 LIDDELL HART i. m. . p. 493.

20 A megfigyelés szakaszában a döntéshozó információkat gyűjt a döntéshozatali folyamat által érintett jelenségről/helyzetről/állapotról. Fontos megemlíteni, hogy a döntéshozatal ezen szakaszban mind az információkat összegyűjtő érzékszervek, szenzorok és elektronikus rendszerek, mind pedig a megszerzett információk támadhatók információs eszközökkel. A második lépésben kiértékelésre kerülnek a megszerzett új információk, amik először az előzetes tudásanyaggal kerülnek összevetésre, majd beépülnek a környezetről meglévő ismeretek közé. A modell az új információk beépítése során kiemelt fontosságot tulajdonít az előzetes tapasztalatoknak, kulturális tradícióknak, szokásoknak, valamint az információkat kiértékelő és szintetizáló módszereknek. A kiinduló ismeretek ugyanis meghatározhatják, hogy a döntéshozók miként értelmezik az új eseményekről szóló információkat. Boyd szerint az orientációs szakasz jelenti az egész OODA ciklus súlypontját. Bővebben lásd: BRUMLEY, L.– KOPP, C. – KORB, K.: The Orientation step of the OODA loop and Information Warfare, Monash University, Australia, Clayton School of Information Technology, 1991. p. 18.

21 Boyd eredetileg egy olyan modellt akart alkotni, mellyel képes elemezni a pilóták légiharc alatti döntéshozatali folyamatát, majd ebből később ezt egy általános elméletet alkotott. Bővebben uo.: p. 18.

megtévesztésre, valamint a kulturális és pszichológiai hatások kihasználására. Boyd felfogásában a legfőbb cél tehát a döntések gyors végrehajtása és a kezdeményezés megragadása, ezzel párhuzamosan be kell hatolni az ellenség OODA ciklusába, össze kell zavarni a vezetési és irányítási rendszerét, azaz ki kell billenteni az egyensúlyi helyzetéből.[22] Az OODA ciklus elmélete később jelentős hatást gyakorolt az amerikai haderő doktrínáira és elképzeléseire, valamint az információs műveletek koncepciójára.

Összefoglalásképp elmondható, hogy az indirekt stratégiák évszázadok óta a hadviselés szerves részét képzik, de csak az elmúlt évek technológiai fejlődése tette lehetővé, hogy helyettesíteni tudják a direkt – katonai – eszközöket és stratégiai hatásokat tudjanak kiváltani. A változások megértéséhez előbb röviden áttekintem a történelem nagy technológiai-társadalmi változásait.

a. Az ipari korszak háborúitól az információs korszak hadviseléséig

A háború mindenekelőtt társadalmi jelenség, melyre az adott korszak technológiai-társadalmi viszonyai gyakorolják a legnagyobb hatást. A téma szempontjából szükséges, hogy röviden kitérjek az emberi társadalmak fejlődésének kérdésére, melyhez Alvin Toffler amerikai társadalomtudós és futurológus 1980-ban megjelent *„Harmadik hullám”* című munkáját vettem alapul.

Toffler a történelem forradalmi jelentőségű technológiai és társadalmi változásait alapul véve, három egymást követő korszakra – hullámra – osztotta fel az emberi társadalmak történetét. Az első hullámban a neolitikus korszak végén egy mezőgazdasági forradalom ment végbe Mezopotámia és Egyiptom területén, melynek köszönhetően művelés alá vonták a földeket, kialakultak az első városok – és velük eljött az emberi civilizáció hajnala. Az ezt követő második hullám csak évezredekkel később, az Európában kibontakozó újabb technológiai forradalom után indult meg, mely az ipari társadalmak megjelenéséhez vezetett a XVIII-XIX. században. Az iparosodást és gépesítést követő újabb nagy ugrást az információs technológiák rohamos fejlődése hozta magával, melynek eredményeképp a hidegháborús korszak második felében megnyílt az út a harmadik hullám előtt. E folyamatokból Toffler azt a következtetést vonta le, hogy mindez egy újabb – információs – technológiai forradalmat fog eredményezni a világ fejlett országaiban, melynek köszönhetően létre fognak jönni az információs társadalmak. A szerző úgy érvelt, hogy az információ a politikai, társadalmi, gazdasági és tudományos élet alapvető erőforrásává fog válni, és olyan központi szerepet fog játszani a jövő új típusú technológiai társadalmaiban, mint amilyet az acél, a szén vagy az olaj játszott az ipari társadalmak korában.[23]

A szerző legfontosabb megállapítása, hogy az információra épülő technológiák forradalma a hidegháború végére megteremtette a feltételeket az emberi történelem harmadik nagy korszakának – hullámának – kibontakozásához, melynek hatására egy mélyreható és gyökeres változás fog megindulni – és létrejönnek az információs társadalmak. Mindez a hadviselés terén is jelentős változásokat fog okozni, ami

---

[22] KRAJNC Zoltán: A légierő mint eszmerendszer, http://legiero.blogspot.hu, 2009. (Letöltés ideje: 2018. 04. 25.)

[23] TOFFLER, Alvin: A harmadik hullám, Budapest, Typotex, 2001. pp. 236-237., p. 351.

fokozatosan átalakítja a fegyveres erők eszközrendszerét, felépítését, valamint a katonai műveletek céljait és tervezését.[24] Ez egy jelentős paradigmaváltásként értelmezhető, mivel a korábbi évszázadok nyugati hadművészetében az ellenséges erők fizikai megsemmisítését célzó direkt hadviselés számított a fegyveres küzdelem domináns formájának.[25]

A direkt katonai eszközökre építő szemléletmód a hidegháború második felében – elsősorban nyugaton – kezdett megváltozni az információs technológiák terén elért robbanásszerű fejlődéssel. Ennek eredményeképp megszületett egy új katonai-technikai forradalom, melynek középpontjába a nagy pontosságú fegyverrendszerek, az űrbázisú-, valamint az egyéb elektronikus felderítő és megfigyelő eszközök, az automatizált vezetési és irányítási, valamint kommunikációs és informatikai rendszerek kerültek. Ezen eszközök tömeges alkalmazására és az új szemléletmódot tükröző műveleti tervezési koncepció első debütálására az 1991-es Öböl-háborúban került sor. Mindez egy teljesen új korszak előszele volt, ami demonstrálta a hadviselés terén végbement gyökeres változásokat.[26]

A változások először leginkább a légierőt érintették, az egyik legfontosabb újdonság pedig a katonai műveletek megtervezése és a célpontok kiválasztása terén jelentkezett. John Warden, az amerikai légierő ezredese elévülhetetlen érdemeket szerzett a párhuzamos háború elmélet (Parallel Warfare), az ellenség, mint rendszerkoncepció (enemy as system) és az „öt gyűrűs" célpont-kiválasztási modell kidolgozásával. Warden egy olyan új célpont-kiválasztási modellt alkotott meg 1995-ös írásában,[27] mely az ellenséget egy összekapcsolt rendszerként értelmezi.

A társadalom stratégiai fontosságú alrendszereit öt koncentrikus körrel rajzolta fel, melynek legbelső magjában a politikai vezetés kapott helyet, amit belülről kifelé haladva a gazdaság működtetéséhez nélkülözhetetlen alrendszerek, az infrastruktúra, a lakosság, végül pedig a legkülső gyűrűben elhelyezkedő haderő követ. Warden

---

[24] A Sivatagi Vihar hadművelet tanulságaiból kiindulva Toffler amellett foglalt állást, hogy a jövőben a fegyveres erők szervezeti felépítése is át fog alakulni, mivel az új, nagy pontosságú fegyverrendszerek, a korszerű harctéri információs hálózatok és a fejlett felderítő rendszerek hadrendbe állításának köszönhetően jelentősen megnő a fegyverek pontossága és tűzereje, így a kijelölt célpontok megsemmisítése kevesebb erő bevetésével is elérhető lesz a jövőben. TOFFLER Alvin – TOFFLER Heidi: War and Anti-War: Making Sense of Today's Global Chaos, Grand Central Publishing, 1995. p. 72-89.

[25] A hadviselés e formája az ipari korszakban ért csúcspontjára olyan koncepciókat hozva létre, melyek a tűzerő folyamatos növelésére, az erők és eszközök koncentrálására, valamint a csapatok manővereire helyezték a hangsúlyt. A győzelem gyors kivívása érdekében a teljes társadalmat és gazdaságot mozgósították, nagy létszámú tömeghadseregek jöttek létre és minden erőforrás a háborús céloknak lett alárendelve, más szóval a háború is „ipari méreteket" öltött.

[26] A fejlett informatikai rendszerek és szenzorok révén a 21. században kezd megvalósult a hálózat alapú hadviselés, melyben a politikai és katonai döntéshozatali rendszer, valamint a hadszíntéri végrehajtó rendszer egy valós idejű hálózatba szerveződik. Mindez jelentősen lerövidíti a reakcióidőt, növeli a műveleti hatékonyságot, melynek köszönhetően a kitűzött célok kevesebb erő bevetésével hajthatóak végre. SZABÓ József: Kis magyar hadelmélet, illetve mire készítsük fel a honvédtiszteket a XXI. században, Hadtudományi Szemle, 2012. V. évf. 3-4. sz. pp. 378-384.

[27] WARDEN John: Air Theory for the Twenty-First Century, Airpower Journal, 1995.

szerint a célpontok kiválasztásánál törekedni kell rá, hogy azok lehetőleg minél közelebb legyenek a stratégiai fontosságú centrumhoz, így a légierő által végrehajtott csapások lehetővé teszik a kívánt végállapot gyors elérését és az adott konfliktus lezárását.

A szemben álló fél stratégiai súlypontjaira (Center of Gravity – COG)[28] mért összehangolt, tömeges és egyidejű mélységi csapásokkal megbénítható a központban elhelyezkedő vezetési és irányítási rendszer, ami megzavarja az egyes alrendszerek rendeltetésszerű működését, elérve a stratégiai bénítást (strategical paralysis). A műveletek tervezése során a belülről-kifelé és nem a kívülről-befelé elv érvényesül, azaz a központi alrendszerek támadásával elérhető az ellenség ellenállóképességének megtörése. A támadások végrehajtása során kiemelt szerep hárul a légierő nagy pontosságú – precíziós – fegyverrendszereire, valamint a C4ISR rendszerekre. A tervezés során először az elérni kívánt végállapotot kell meghatározni, ezt követően azonosítani kell az ehhez szükséges stratégiai súlypontokat, melyek bénításához további célpontok kijelölésére van szükség.[29]

A modell megalkotásának idején a stratégiai bénítást csak kinetikus eszközökkel – a légierő által végrehajtott mélységi csapásokkal – lehetett kiváltani. Ebben az időszakban még nem épült ki az az átfogó információs infrastruktúra, ami biztosítja a különböző alrendszerek működését és a közöttük folyó információáramlást.

Ezek megjelenésével és az információs társadalmak létrejöttével párhuzamosan a stratégiai hadviselés terén is forradalmi változások következtek be a 20. század utolsó évtizedében, melynek hatására megszületett a stratégiai információs hadviselés koncepciója.

b. A stratégiai információs hadviselés kialakulásának oka

Az információtechnológia dinamikus fejlődése lehetővé tette a számítási feladatok és a logikai műveletek végrehajtási teljesítményének folyamatos növekedését és az IKT eszközök széleskörű elterjedését, melynek köszönhetően jelentősen megnőtt a szükséges információk előállításának, feldolgozásának, tárolásának és továbbításának hatékonysága. Ennek köszönhetően az információs társadalmakban drasztikus mértékben felgyorsult az információáramlás,

---

[28] A stratégiai súlypont az ellenség alrendszereinek olyan jól meghatározott középpontja, melynek megbénítása esetén a többi alrendszerben olyan zavarok keletkeznek, melyek megbénítják a szemben álló fél teljes társadalmát. Bővebben lásd: KRAJNC Zoltán – GÖNCZI Gabriella: Korunk meghatározó légierő teoretikusa: John A. III. Warden, Hadmérnök, V. évf. 1. sz. 2010. p. 355.

[29] Warden ellenség, mint rendszer és öt gyűrűs modelljének továbbfejlesztésével később létrejött az úgynevezett hatásalapú műveletek (Effect Based Operations – EBO) koncepciója. Ennek lényege, hogy a kívánt végállapot eléréséhez a közvetlen hatások – egy adott célpont elpusztítása – helyett a másod- és harmadlagos – közvetett – hatások kiváltására kerül a hangsúly, amit összehangolnak a kívánt végállapottal. A hatásalapú műveleteknek nincs egységes definíciója, leginkább egy szemléletmódként és tervezési módszertanként lehet értelmezni. Bővebben lásd: KRAJNC Zoltán – GÖNCZI Gabriella: A légi hadjáratok (műveletek) stratégiai szintű tervezésének és az üzleti (vállalati) stratégiaalkotásnak a konvergenciája (egy. PhD-témaválasztás indoklása) Szolnok, Repüléstudományi Konferencia, 2009. p. 10.

hozzájárulva a gazdasági fejlődéshez, valamint az állami, katonai, technológiai, társadalmi stb. szektorok gyorsabb és hatékonyabb működéséhez. E folyamat azonban számos előnye mellett[30] együtt jár az információs rendszerektől és szolgáltatásokról való nagyfokú függőség, valamint olyan kiszolgáltatottság kialakulásával, ami egyúttal új sebezhetőségeket, továbbá biztonsági kihívásokat, kockázatokat, fenyegetéseket jelentenek az államok számára. Az országok létfontosságú rendszerei és létesítményei[31] – energiaellátás, távközlés, egészségügy, jogrend, bankrendszer, közbiztonság, honvédelem stb. – szempontjából ugyanis létfontosságú az információs rendszerek és infokommunikációs infrastruktúrák zavartalan, folyamatos működésének biztosítása, melyek meghibásodása, kiesése vagy tartós leállása esetén akár az egész állam összeomolhat.[32]

Mindez azt jelenti, hogy az állami információs rendszerek (hardverei és szoftverei) ellen indított összehangolt támadássorozattal egy adott ország kritikus infrastruktúrái időlegesen megbénulhatnak, vagy tartósan leállhatnak, melynek hatására működésképtelenné válhatnak az alapvető állami, gazdasági, társadalmi stb. funkciók és szolgáltatások. A támadások az információs környezet valamennyi – fizikai, kiber, elektromágneses és kognitív – tartományban[33] bekövetkezhetnek, ezért a védekezésnek ki kell terjednie az információs rendszerek fizikai és logikai[34] védelmére, valamint a kognitív dimenzióban[35] folyó információs folyamatok ellenőrzésére, hogy semlegesíteni lehessen a támadó fél manipulációs és befolyásolási kísérleteit.

---

30 Gondoljunk csak a széleskörű webes szolgáltatások jelentette kényelemre – elektronikus közigazgatási szolgáltatások, banki ügyintézés, online vásárlás, kapcsolattartás és kommunikáció, információszerzés, távoktatás és távmunka stb.

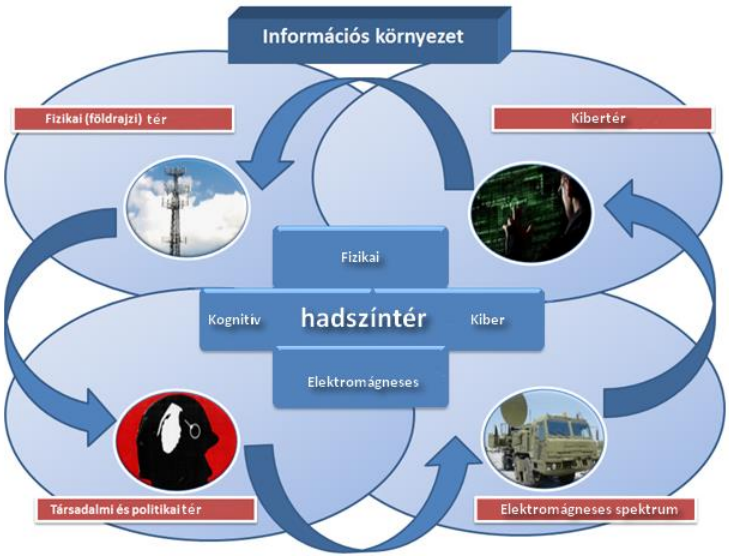
31 A részletes felsorolást a magyarországi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény tartalmazza. Bővebben lásd: 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,

32 Krasznay Csaba és Kovács László *Digitális Mohács* címmel megjelent tanulmányukban egy ehhez hasonló forgatókönyvet vázoltak fel, melyben bemutatták egy Magyarország ellen irányuló, átfogó kibertámadás lehetséges következményeit. Bővebben lásd: KOVÁCS László – KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság1. sz. 2017.

33 Az információs környezet különböző tartományainak egymáshoz való viszonyáról lásd: 1. ábra

34 Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem, amelynek fontosabb részei az azonosítás és a hitelesítés, a hozzáférés-védelmi rendszer, a bizonyítékok rendszere. Forrás: MUHA Lajos (szerk.): Az informatikai biztonság kézikönyve – Informatikai biztonsági tanácsadó A-tól Z-ig, Verlag Dashöfer Szakkiadó, 2000-2005.

35 A kognitív hadszíntér vonatkozásában több utalást is találhatunk a szakirodalomban, melyek az információs műveletek egyik működési tartományaként hivatkoznak rá. Jelen tanulmányban a kognitív hadszíntér alatt a konfliktusok egy olyan különleges tartományát értem, ahol a szemben álló felek komplex befolyásolási műveleteket folytatnak a közvélemény összezavarása, manipulálása és megnyerése érdekében, ezzel biztosítva a stratégiai célok elérését. Bővebben lásd: FEKETE Csanád: Információ és hadviselésháború a kognitív hadszíntéren II., Szakmai Szemle 4. sz. 2016. pp. 51-55.



1.ábra: Az információs hadviselés működési tartományai
(saját szerkesztés)

c. A stratégiai információs hadviselés színre lépése

A legjelentősebb nyugati kutatók – John Arquilla és David Ronfeldt, Winn Schwartau, Alvinés Heidi Toffler, Roger C. Molander, Martin Libicki, Richard Szafranski – az információs technológiák rohamos fejlődéséből és az ennek hatására jelentkező politikai, társadalmi, gazdasági és tudományos trendekből azt a következtetést vonták le, hogy azok hadviselésre gyakorolt hatásai olyan forradalmi változásokat fognak előidézni, mint amelyeket az Öböl-háború esetében tapasztalhattunk.[36] A szerzők egy része szerint az információs térben folytatott küzdelem egyre inkább stratégiai jelentőséget fog játszani a jövőben. Így az a hadviselő fél, amelyik egy adott konfliktusban képes megszerezni és megtartani az információs fölényt, behozhatatlan előnyre tesz szert, így clausewitz-i értelemben könnyedén rá tudja kényszeríteni akaratát a szemben álló félre. Egyes szakértők[37] ennél is továbbmentek, és az információs tér meghatározó stratégiai jelentőségét hangsúlyozták. Ennek eredményeképp a RAND kutatóintézet munkatársai megalkották a stratégiai információs hadviselés koncepcióját.

A RAND Corporation 1995-ben nemzetbiztonsági és civil szakemberek bevonásával egy olyan gyakorlatot végzett, melyben több olyan lehetséges

---

[36] Az Öböl-háború sokak szerint átmenetet képez a hagyományos felőrlő jellegű ipari hadviselés és az információs korszak hadviselése között. ARQUILLA John: The Advent of Netwar, RAND Corporation, 1996. p. 104.

[37] Nyugaton többek között John Arquilla és David F. Ronfeldt foglalkozott sokat a témával, olyan nagy hatású könyveket adva ki, mint az 1996-ban megjelent „*The Advanet of Netwar*" vagy a 2000-es „*Swarming and the Future of Conflits.*" Ezekről bővebben lásd: ARQUILLA John – RONFELDT David F.: Swarming and the Future of Conflits., RAND Corporation, 2000; ARQUILLA John: The Advent of Netwar, RAND Corporation, 1996

forgatókönyvet vizsgáltak, melyben az Egyesült Államok és szövetségesei ellen információs támadást[38] hajtottak végre. A gyakorlat tapasztalatairól *„Stratégia információs hadviselés: a háború új arca”* címmel egy tanulmányt[39] adta ki, melyben felhívták a figyelmet az információs hadviselés által jelentett fenyegetésekre. Az 1996-os írásban 7 olyan fontos tényezőt és problémát emeltek ki, melyek szerintük a stratégiai információs hadviselés jellemzik:

- alacsony költségek,
- egymásba mosódó határvonalak – külső és belső elkövetők, aktorok,
- a percepció menedzsment növekvő szerepe,
- a stratégiai hírszerzés új kihívásai,
- a támadások előrejelzésének és a támadások értékelésének problémái,
- a koalíciók létrehozásának és fenntartásának nehézségei,
- az Egyesült Államok sebezhetősége.

A stratégiai információs hadviselés a szerzők szerint az államok és nem állami szereplők eszköztárának fontos eszközévé fog válni a jövőben, kiegészítve az információs eszközökkel rendelkező fejlett konvencionális erőket, valamint a tömegpusztító – nukleáris, biológiai, vegyi – fegyvereket. [40]

A szerzők megállapításai álláspontom szerint megelőzték korukat és helytállónak bizonyultak. Azt azonban ők sem láthatták előre, hogy a 2000-es évek egyre gyorsuló fejlődése – internet felhasználók dinamikus növekedése, hordozható és „okos” infokommunikációs eszközök tömeges elterjedése – egy új szintre fogja emelni a kognitív térben folyó küzdelmet, amit az „Iszlám Állam” elnevezésű terrorszervezet megjelenése, és az egyre nagyobb figyelmet kapó orosz információs műveletek is jól mutattak.[41]

Az elmúlt időszak konfliktusai rávilágítottak a kognitív hadszíntéren folyó befolyásolási műveletek egyre növekvő szerepére. A 2000-es évek NATO szerepvállalásaiból – és a 2014-es ukrán válságból – levont tanulságok hatására konkrét lépések történtek annak érdekében, hogy a NATO megfelelő választ adjon ezen kihívásokra. Ennek részeként 2014. július 1-jén, Rigában létrehozták a NATO Stratégiai Kommunikáció Kiválósági Központját[42], melynek feladata, hogy összehangolja azon tagállami erőfeszítéseket, melyek az információs térből érkező káros befolyásolási műveletek elhárítására irányulnak. Ezen felül a különböző kormányzati és önálló kezdeményezésű polgári szervezetek, kutatóközpontok, valamint a technológiai szektor jelentős képviselői is összefogtak annak érdekében, hogy felderítsék, illetve kiszűrjék az állami és más felelősségű résztvevőktől – mint például a nemzetközi terrorszervezetektől vagy szervezett bűnözői csoportoktól –

---

38 Információs támadás alatt olyan szervezetten és összehangoltan végrehajtott műveleteket értek, melyek párhuzamosan folyhatnak az információs környezet egynél több tartományában.

39 MOLANDER Roger C. – RIDDILE Andrew – WILSON Peter A.: Strategic Information Warfare - A New Face of War, RAND Corporation, 1996.

40 Uo. pp. 1-3.

41 FEKETE Csanád: Információ és hadviselés – háború a kognitív hadszíntéren II. Szakmai Szemle, 2016, XIV. évf. 4. sz. pp. 46-80.

42 Seven Allies Establish NATO's Strategic Communications Center of Excellence in Latvia, NATO STRATCOM, 2014.

származó fenyegető, valótlan és megtévesztő információkat, az álhíreket, a propagandaanyagokat és az egyéb félrevezető, káros információkat.[43]

A stratégiai információs hadviselés tehát ötvözi a technika-központú kibertér-műveleteket és a kognitív térben folyó befolyásolási műveleteket. Az előbbi a célország információs rendszereibe történő behatolással, az információk kinyerésével és konfliktus esetén az információs infrastruktúrák megbénításával, míg az utóbbi a lakosság manipulálásával, a döntéshozatali rendszer összezavarásával és társadalmi rend aláásásával foglalkozik.

A *„Stratégiai információs hadviselés"* legfőbb előnye a stratégiai célok katonai erő speciális, közvetett hatású alkalmazásában rejlik. A földrajzi tér ellenőrzése és az ellenség fizikai pusztítása helyett (direkt megközelítés) az információs fölény kivívása és a stratégiai súlypontok információs eszközökkel történő támadása (indirekt megközelítés) kerül a középpontba, melynek célja a stratégiai bénítás kiváltása és a végállapot elérése minimális kinetikus eszköz igénybevételével. A korábbi korszakokhoz képest további változást jelent, hogy az információs korszak stratégiai súlypontjai az információs infrastruktúrák lettek, így ezek támadásával – minimális fizikai károkozás mellett – elérhető a stratégiai bénítás és az ellenség akaratának megtörése. A *Stratégiai információs hadviselés* egy olyan átfogó rendszert alkot, ami számos szempontból megkülönböztethető a hadviselés többi formájától, amit az alábbi táblázatban foglaltam össze:

Stratégiai információs hadviselés	
Célok	A másik fél stratégiai pozícióinak gyengítése, a politikai rendszer megdöntése, társadalmi és politikai válság előidézése, a döntéshozatali rendszer megbénítása, stratégiai bénítás kiváltása
Célpontok	Döntéshozók, lakosság, információs rendszerek és létfontosságú infrastruktúrák
Eszközök	Információs fegyverek,[44] automatizált szoftveres alkalmazások,[45] a hírszerzés klasszikus eszközei
Résztvevők	Államszint alatti szereplők, államilag szponzorált hackercsoportok, a fegyveres erők kiberalakulatai, titkosszolgálatok, egyéb állami és nem állami szervezetek stb.
Módszerek	Befolyásolási műveletek, kibertér-műveletek
Működési környezet	Az információs környezet különböző dimenziói: kibertér, elektromágneses spektrum, fizikai közeg, kognitív közeg

[43] NICK Newman: Overview and Key Findings of the 2017 Report, Digital News Report, 2017

[44] Beleértve a kiberfegyvereket és az egyéb olyan technikai megoldásokat, mint az elosztott túlterheléses támadások (DDoS), vagy a troll hadseregek.

[45] A jövőben kiemelten fontos lesz a gépi tanuláson nyugvó megoldások alkalmazása. Ezek lehetőségeiről lásd: ANDERSON Berit – HORVATH Brett: The Rise of the Weaponized AI Propaganda Machine There's a new automated propaganda machine driving global politics. How it works and what it will mean for the future of democracy., Scout, 2017.

d. Az információs tér stratégiai jelentősége napjainkban

A folyamatosan fejlődő technológiának köszönhetően az összehangolt információs támadások mára az államok és állami szint alatti szereplők érdekérvényesítésre szolgáló olyan erőszakos eszközévé vált, mely alkalmazása – az ellenség kritikus infrastruktúrája súlypontjai ellen indított összehangolt információs támadások – révén megvalósíthatók a kitűzött stratégiai célkitűzések.

Egyesek amellett érveltek, hogy a hadviselés egy olyan új formájaként foghatók fel a politikai célok érdekében indított kibertér-műveletek,[46] melyek nehezen illeszthetők be a korábbi hadviselési formák hagyományos eszköztárába. Az információs küzdelem részének tekinthető kibertér-műveletek az állami erőszak alkalmazásának egy olyan új formáját jelenthetik, ami közvetlenül ugyan nem tekinthető halálosnak, de az okozott károk és közvetett hatások hatalmas veszteséget és társadalmi problémákat jelenthetnek.

Az elmúlt évek tapasztalatai alapján megállapítható, hogy az információs korszak összetűzései, „háborúi" egyre inkább a kiber- és kognitív tartományban fognak folyni a lakosság, valamint a döntéshozók befolyásolásáért és nem utolsó sorban az információs folyamatok ellenőrzéséért. Mindez azt eredményezheti, hogy a konvencionális erőfölény megléte önmagában nem lesz elegendő a stratégiai célok eléréséhez. Az a fél, amelyik megnyeri az információs térben folytatott harcot, az érdemben tudja csökkenteni a másik fél társadalmi támogatását és megzavarhatja a döntéshozatali folyamatait, megtagadva a szemben álló féltől a „háború" folytatásához szükséges információs erőforrásokat.

Tofflert némileg igazolva az információ olyan kritikus erőforrássá változott napjainkban, ami képes akár egy fegyveres konfliktus kimenetelére is hatással lenni. Izrael hiába élvezett jelentős katonai fölényt a 2006-os libanoni háború vagy a 2014-es gázai konfliktus során, a kognitív tartományban folyó „propagandaháborút" elvesztette és ennek hatására le kellett állítania a katonai műveleteket. Ebből is látható, hogy az aszimmetrikus konfliktusokban az információs folyamatok ellenőrzése kritikus fontosságú, mely révén biztosítható a kellő társadalmi támogatottság, illetve a helyi lakosság bizalmának elnyerése.[47]

Ebből levonható az a következtetés, hogy a modern technológia és az információs eszközöknek köszönhetően a nem állami szereplők – valós katonai képességek nélkül is – sikerrel tudják felvenni a harcot az államokkal szemben. A nyugati államokra nézve az egyik legnagyobb jövőbeni fenyegetést a társadalom percepcióit célzó befolyásolási műveletek, és az indirekt módszerekre építő aszimmetrikus stratégiák kombinációja jelenti.[48] A támadó fél manipulációs technikák alkalmazásával anélkül kényszeríthetné rá akaratát az adott országra, hogy annak tényleges katonai potenciáljára nem mér közvetlen csapást. A közvélemény befolyásolásával ugyanis megtörhető a háború folytatásához fűződő politikai akarat, ahogy azt az Egyesült Államok 1994-es szomáliai tapasztalatai is megmutatták.

---

[46] RATTRAY Gregory J.: Strategic Warfare in Cyberspace, MIT Press, 2001. p. 20.

[47] Bővebben lásd: CONGER George: Study: Hizbullah won propaganda war, The Jerusalem Post, 2007.

[48] Lásd a hibrid hadviselés koncepcióját. Bővebben: FEKETE Csanád: A hibrid hadviselés elméleti kérdései, Nemzeti Közszolgálati Egyetem, 2016.

Gondolatok a hadügyi paradigmaváltásról

A cikk elején feltett első kérdésre adható válaszban egy új paradigma és hadügyi forradalom kialakulására nem felelhetünk egyértelműen igennel. Egy átmeneti korszakban vagyunk, melyben a forradalmi változások beindultak, a nem-kinetikus – köztük elsősorban az információs – eszközök stratégiai jelentőségre tettek szert, de a fegyveres erő továbbra is az államok érdekérvényesítési eszköztárának fontos részét képezik. Ezzel kapcsolatban fontos tisztázni mit tekinthetünk forradalomnak és mit evolúciónak. A hadtudományi lexikon meghatározása szerint *„a hadügy fejlődésében evolúciós és revolúciós szakaszokat lehet megkülönböztetni. A hadügy forradalmairól akkor lehet beszélni, ha annak egészében és minden alapvető elemében gyökeres, új minőséget képviselő változás bontakozik ki. A fentiekből következik, hogy a hadügy forradalmán a fegyveres erők szervezetében, kiképzésében és nevelésében, a hadviselés módjaiban, a fegyveres harc eszközeiben, valamint az ország (szövetség) felkészítésében végbement minőségi változások összességét értjük."* [49]

A hadügyi forradalom kapcsán a haditechnikai fejlődés mellett fontos figyelembe venni az emberi tényező szerepét is. A két tényező egymásrautaltsága az elmúlt két évtized forradalmi változásaiban is tetten érhető, az egyre fejlettebb fegyverrendszerek alkalmazása döntő mértékben befolyásolja a harcok menetét, és lehetővé teszik a győzelem kivívását, de azt csak a magasan képzett, az adott technikához értő professzionális katonákkal együtt lehet valóra váltani. Emellett a politikai és társadalmi változásokat sem lehet figyelmen kívül hagyni, a bipoláris világrend megszűnését követően alapvetően megváltoztak a hatalmi viszonyok, ami a hadügyben is változásokat idézett elő.

A hidegháborús korszakban, majd a Szovjetunió szétesését követően az új posztbipoláris korszakban a hangsúly a prevencióra és a válságreagálásra helyeződött át. A katonai műveletekben fokozatosan háttérbe szorult a fegyverhasználat, a komplex természetű konfliktusok kezelésében pedig az erőkivetítés kérdése, valamint a katonai erő indirekt oldalának alkalmazása és a polgári együttműködés jelentősége növekedett. A hadügy alkalmazkodva az új környezethez, napjainkban egyrészt az új típusú biztonsági kihívásokra történő felkészülésre, valamint a hadügyi forradalom keretében megvalósuló tudományos-technikai fejlődés vívmányainak felhasználására fókuszál. Legfőbb célja pedig a honvédelem hagyományos feladatainak megszervezése és ellátása mellett az új biztonsági környezethez igazodó, korszerű haderő kialakítása – transzformációja – lett.

A hidegháború éveiben a haditechnikai fejlesztések eleinte a nukleáris és tömegpusztító fegyverekre – valamint azok hordozóeszközeire –, majd a konvencionális fegyverek új generációjának folyamatos fejlesztésére és hadrendbe állítására irányultak, megnyitva az utat az új tudományos-technikai forradalom előtt.[50] Az utóbbi forradalom középpontjában az információs technológiák állnak,

---

[49] SZABÓ József (szerk.): Hadtudományi lexikon I., Budapest, Magyar Hadtudományi Társaság, 1995. p. 480

[50] Project Solarium néven az első offset stratégia még 1950-ben került meghirdetésre, mely a nukleáris technológiák terén meglévő amerikai fölényre épült. A '80-as években kibontakozó második offset stratégia célja a szovjetek konvencionális katonai fölényének

melyek fejlődése véleményem szerint mára az emberi történelem egy teljesen új, információs korszakát is elhozták. Ennek figyelembevételével a XX. században az alábbi hadügyi forradalmak mentek végbe, melyek mind meghatározók voltak a hadviselés tekintetében: gépesített háború – rakéta-atomháború- információs háború.

A jelenleg kibontakozó újabb evolúciós szakaszban az emberi tényező kiváltására helyeződik a hangsúly az új autonóm fegyverrendszerek és katonai robotok megjelenésével. A hadtudományi lexikon szerint: „*A magas, csúcstechnológiai színvonalú fegyverek és eszközök katonai alkalmazása új módon veti fel, de nem csökkenti az ember szerepét. Minél nagyobb a harceszközök pusztítóereje és bonyolultsága, valamint a csapatok technikai ellátottsága, gépesítése és az automatizáltság, annál bonyolultabb és fontosabb az ember szerepe a harc megvívásában.*"[51]

A konvencionális katonai erő napjainkban már nem számít a stratégiai kelléktár elsődleges elemének, ennek ellenére szerepe a jövőben is meghatározó marad az akarat kikényszerítésének „ultima ratio" eszközeként, de felépítése, szerkezete, eszközrendszere – az újabb evolúciós szakaszban – várhatóan további nagy átalakuláson fog keresztül menni a szuperszonikus rakétarendszerek, az irányított energiájú fegyverrendszerek, valamint a robotika, és a mesterséges intelligencia egyre nagyobb térnyerésével. Végül megállapítható, hogy az ipari korszak konfliktusaihoz képest a 21. századi hadviselésének sebessége drasztikus mértékben felgyorsult, amit percekben és órákban lehet kifejezni. William C. Hix amerikai ezredes egy konferencián az alábbiakban fogalmazta meg mindezt:
„A jövő háborúja gyors és halálos lesz….az automatizált fegyverrendszerek és a mesterséges intelligencia soha sem látott mértékben gyorsítja fel a harcok menetét... az események gyorsasága várhatóan meg fogja haladni az emberi elme felfogóképességét;"[52]

Összegzés

Az elmúlt évek eseményei alapján kijelenthetjük, hogy egy olyan átmeneti korszakban élünk, ahol az információs környezetben folytatható műveletek egyre jobban meghatározzák a konfliktusok kimenetelét, de még továbbra is jelentős marad a szerepe az állami, katonai eszközöknek és a hagyományos kinetikus műveleteknek. Az információs korszak már eddig is olyan jelentős változásokat hozott a hadviselés terén, melyek alapján egyes elméletek – mint például a hibrid

minőségi tényezőkkel – például a nagy pontosságú fegyverrendszerek és felderítő eszközök kifejlesztésével – történő ellensúlyozása volt. A témával magyar nyelven részletesen foglalkozott Porkoláb Imre dandártábornok, a NATO Szövetséges Transzformációs Parancsnokság Pentagoni összekötő irodájának vezetője. Lásd: PORKOLÁB Imre: Innováció – A jövő hadviselésének meghatározó eleme a változó környezetben, in: Felderítő Szemle, 2015. 14. évf. 3. sz.

51 SZABÓ József (szerk.): Hadtudományi lexikon I., Budapest, Magyar Hadtudományi Társaság, 1995. p. 482.

52 PENSITON Bradley: Army Warns that Future War with Russia or China Would Be 'Extremely Lethal and Fast', Defense One, 2016.

vagy a korlátok nélküli hadviselés – az indirekt stratégiák, és a nem-katonai eszközök konfliktusokban játszott szerepének felértékelődését emelték ki. [53]

A „stratégiai információs hadviselés" fogalmának befogadása révén szemléltethető a kiber- és kognitív tartomány szerepének felértékelődése. A stratégiai információs hadviselés az információs műveletek hagyományos megközelítésével szemben egy jóval szélesebben értelmezett jelenséget ölel át, ami nagyban segíti az elmúlt évek eseményeinek – többek között az amerikai elnökválasztási kampány, valamint az orosz dezinformációs műveletek – pontosabb megértését és a tapasztalatok feldolgozását is. Amíg az információs műveletek koncepciója a háborús időszakokra terjednek ki, addig a nagyhatalmak között folyó „stratégia információs hadviselés" a béke és a háborús időszakra egyaránt értelmezhető. A taktikai szintű információs műveletek mellett a hálózat alapú hadviselés fejlődése teret adhat a stratégiai jelentőségű hatások kiváltására alkalmas katonai elgondolások megvalósítására is.

A *„stratégiai információs hadviselés"* keretei között a békeidőben a főbb célok közé tartozik az információs folyamatok ellenőrzése, a másik fél információs rendszereiben rejlő sebezhetőségek felderítése, az ellenség társadalmi rendjének aláásása, döntéshozatali rendszerének összezavarása, a konfliktus kirobbanását követően pedig a stratégiai bénítás elérése. Az információs rendszerektől való egyre nagyobb függés egyben azt is jelenti, hogy az a fél, amelyik képes lerombolni vagy megbénítani a másik oldal információs infrastruktúráját és eközben megvédeni a sajátját, az döntő stratégiai fölényre tehet szert egy fegyveres konfliktusban. Aki nem alkalmazkodik az információs korszak megváltozott körülményeihez és adaptálódik az információs hadviselés jelentette kihívásokhoz, az alul fog maradni a jövőben.

Kulcsfontosságú, hogy az információs térben zajló események folyamatos megfigyelés alatt álljanak, mivel egy a kibertérből kiinduló összehangolt hatására leállhatnak az ország létfontosságú rendszerei, megbénulhat a döntéshozatali rendszer, melynek hatására jelentős társadalmi és politikai válság alakulhat ki. A *„stratégiai információs hadviselésben"* központi szerepet játszó befolyásolási műveletek túlmutatnak a kibertér határain, így célszerű az információs tér valamennyi tartományára kiterjedő rendszerszintű megközelítés alkalmazása. A befolyásolási és kibertér-műveletek elhárításához továbbá elengedhetetlen a támadások korai észlelése, a támadó szándékának és stratégiájának azonosítása, valamint egy koherens kommunikációs stratégia kidolgozása.

A *„stratégiai információs hadviselést"* az államok – és államszint alatti szereplők – várhatóan egy olyan költséghatékony és hatásos eszközként fogják használni az államok közötti, valamint az államok működését negatívan befolyásoló konfliktusok esetében, ami fokozni fogja az információs térben zajló küzdelem intenzitását, melyek akár a fizikai tartományra is átterjedhetnek. Az információs műveletek fokozódása miatt az államok alapvető nemzetbiztonsági érdeke, hogy kiemelt figyelmet fordítsanak az információs rendszerek védelmére, melynek

[53] Valerij Geraszimov tábornok 2013-ban megjelent hírhedté vált cikkében úgy fogalmaz, hogy az új típusú konfliktusokban a nem-katonai eszközök 4:1 arányban múlja felül a katonai erőt. Bővebben lásd: GERASZIMOV Valerij: Cennoszty nauki v predvigyenyii, Vojenno-promislennij kurjer, 8. évf. 476. sz. 2013.

keretében elengedhetetlen egy, a lehetséges kockázatokra és fenyegetésekre reflektáló átfogó kibervédelmi stratégia kidolgozása. Az információbiztonság jogszabályi és szervezeti hátterének megteremtése, valamint az ezek implementálásához szükséges források biztosítása nem elégséges a fizikai és logikai téren túlmutató erők leküzdéséhez. A fenyegetések körének bővülése így azt is jelenti, hogy az információs tér komplex megközelítésére van szükség, figyelembe véve a legsebezhetőbb és leginkább támadhatóbb rendszerelemeket, amit a legtöbb esetben a felhasználók és az emberek jelentenek – vagyis a kognitív szféra. Ezért egyrészt szükség van az információbiztonság-tudatosság erősítésére – amit célszerű beemelni például az oktatásba –, másrészt meg kell találni a megfelelő intézkedéseket a befolyásolási műveletek keretében terjesztett propaganda és dezinformációs kísérletek semlegesítésére. Mindez az eddigieknél komplexebb és a biztonság fogalmánál bővebb, átfogó szemléletmódot, továbbá a katonai felfogást egyaránt tartalmazó, védelmi elgondolást kíván.

Felhasznált irodalom:

- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv (Letöltés ideje: 2018. 04. 25.)
- ANDERSON, Berit – HORVATH, Brett: The Rise of the Weaponized AI Propaganda Machine There's a new automated propaganda machine driving global politics. How it works and what it will mean for the future of democracy., 2017, Scout. https://scout.ai/story/the-rise-of-the-weaponized-ai-propaganda-machine (Letöltés ideje: 2018.01. 30.)
- ARQUILLA,, John: The Advent of Netwar, 1996, RAND Corporation
- ARQUILLA, John, RONFELDT, David F.: Swarming and the Future of Conflits., 2000, RAND Corporation
- BRUMLEY L. – KOPP C. – KORB, K.: The Orientation step of the OODA loop and Information Warfare, in: Clayton School of Information Technology, Monash University, Australia, 1991. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=12558E896F6CC83D5630FE248B331D93?doi=10.1.1.159.1144&rep=rep1&type=pdf (Letöltés ideje: 2018. 01. 30.)
- CLAUSEWITZ, Carl V.: A háborúról, Budapest, 2013, Zrínyi Kiadó
- CONGER, George: Study: Hizbullah won propaganda war, in: The Jerusalem Post, 2007. https://www.jpost.com/Israel/Study-Hizbullah-won-propaganda-war (Letöltés ideje: 2018. 04. 10.)
- FEKETE Csanád: A hibrid hadviselés elméleti kérdései: in: KALÓ József (szerk.): Napjaink biztonsági kihívásai, veszélyei és fenyegetései (Tanulmányok a Biztonságpolitikai Szakkollégiumtagjainak írásaiból), 2016, Nemzeti Közszolgálati Egyetem

- FEKETE Csanád: Információ és hadviselésháború a kognitív hadszíntéren I., in: Szakmai Szemle, 2016 3. sz.
- FEKETE Csanád: Információ és hadviselésháború a kognitív hadszíntéren II., in: Szakmai Szemle, 2016 4. sz.
- GERASZIMOV, Valerij: Cennoszty nauki v predvigyenyii., 2013, Vojenno-promislennij kurjer No. 476. http://www.vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf (Letöltés ideje: 2015. 11. 25.)
- HAIG Zsolt: Az információs hadviselés kialakulása, katonai értelmezése, in: Hadtudomány, 2011, 21.évf. 1-2. sz.
- HAIG Zsolt – VÁRHEGYI István: Hadviselés az információs hadszíntéren, Budapest, 2005, Zrínyi Kiadó
- HAIG Zsolt – VÁRHEGYI István: A cybertér és a cyberhadviselés értelmezése, in: Hadtudomány, 2008, 18.évf. E. sz. http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (Letöltés ideje: 2016. 07. 01.)
- KOVÁCS László – KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, in: Nemzet és Biztonság, 2017. 1. sz.
- KRAJNC Zoltán: A légierő mint eszmerendszer, in: http://legiero.blogspot.hu, 2009. http://legiero.blogspot.hu/2009/02/dr-krajnc-zoltan-legiero-mint.html (Letöltés ideje: 2018. 01. 30.)
- KRAJNC Zoltán – GÖNCZI Gabriella: A légi hadjáratok (műveletek) stratégiai szintű tervezésének és az üzleti (vállalati) stratégiaalkotásnak a konvergenciája (egy. PhD-témaválasztás indoklása)., in: Repüléstudományi Konferencia, 2009, Szolnok. http://epa.oszk.hu/02600/02694/00048/pdf/EPA02694_rtk_2009_2_Krajnc_Zoltan-Gonczi_Gabriella_1.pdf (Letöltés ideje: 2018. 01. 30.)
- KRAJNC Zoltán – GÖNCZI Gabriella: Korunk meghatározó légierő teoretikusa: John A. III. Warden, in: Hadmérnök, 2010, V.évf. 1. sz. http://hadmernok.hu/2010_1_gonczi_krajnc.pdf (Letöltés ideje: 2018. 01. 30.)
- LIDDELL HART, Basil H.: Stratégia, Budapest, 2002, Európa Könyvkiadó
- MOLANDER, Roger C.RIDDILE, Andrew, WILSON, Peter A.: Strategic Information Warfare - A New Face of War, 1996, RAND Corporation
- MUHA Lajos (szerk.): Az informatikai biztonság kézikönyve - Informatikai biztonsági tanácsadó A-tól Z-ig, 2000-2005, Verlag Dashöfer Szakkiadó
- NICK, Newman: Overview and Key Findings of the 2017 Report, 2017, Digital News Report. www.digitalnewsreport.org/survey/2017/overview-key-findings-2017/ (Letöltés ideje: 2018. 01. 28.)
- PENSITON, Bradley: Army Warns that Future War with Russia or China Would Be 'Extremely Lethal and Fast', 2016, Defense One. http://www.defenseone.com/threats/2016/10/future-army/132105/ (Letöltés ideje: 2018. 01. 30.)

- PORKOLÁB Imre: Innováció – a jövő hadviselésének meghatározó eleme a változókörnyezetbe, in: Felderítő Szemle, 2015, 14.évf. 3. sz.
- RATTRAY, Gregory J.: Strategic Warfare in Cyberspace, 2001, MIT Press
- Seven Allies Establish NATO's Strategic Communications Center of Excellence in Latvia, NATO STRATCOM, 2014. http://www.atlanticcouncil.org/blogs/natosource/seven-allies-establish-nato-s-strategic-communications-center-of-excellence-in-latvia (Letöltés ideje: 2018. 01. 30.)
- SZABÓ József: Kis magyar hadelmélet illetve mire készítsük fel a honvédtiszteket a XXI. században, 2012, Hadtudományi Szemle pp. 378–384. http://epa.oszk.hu/02400/02463/00013/pdf/EPA02463_hadtudomanyi_szemle_2012_3-4_378-384.pdf (Letöltés ideje: 2015. 11. 24.)
- SZABÓ József (szerk.): Hadtudományi lexikon I., Budapest, 1995, Magyar Hadtudományi Társaság
- SZENES Zoltán: Meglepetések nélkül: A varsói NATO csúcs értékelése, Biztonsagpolitika.hu, 2016
- SZUN-CE: A hadviselés törvényei, Budapest, 1998, Balassi Kiadó
- TOFFLER, Alvin: A harmadik hullám, Budapest, 2001, Typotex
- TOFFLER, Alvin, TOFFLER, Heidi: War and Anti-War: Making Sense of Today's Global Chaos: wj, 1995, Grand Central Publishing
- WARDEN, John: Air Theory for the Twenty-First Century, in: Airpower Journal, 1995

DR. MÓGOR-KRÓZSER TERÉZIA

SZEMÉLYES ADATOK VÉDELMÉNEK FŐ FELADATAI AZ UNIÓS SZABÁLYOZÁS SZEMSZÖGÉBŐL

Az uniós adatvédelmi reform bevezetésével együtt járó változások hatásai, és a Rendelet alkalmazásának előnyei

A GDPR előtti adatvédelmi szabályok[1] bevezetése óta több, mint 20 év telt el, ami az utóbbi évtizedek technikai és technológiai fejlődéséhez viszonyítva rendkívül hosszú időszaknak számított. Az elmúlt két évtizedben létrejött digitális, vezeték nélküli és vezetékes kommunikációs módok lényegesen hozzájárultak ahhoz, hogy az emberek személyes adataikat, információikat napi rendszerességgel és bátrabban osztották meg, mint korábban.

A 2018. május 15-én bevezetett új szabálycsomag nem csak visszaadta a polgároknak a személyes adataik feletti ellenőrzést, hanem számos lehetőséget biztosít a vállalkozások terén is, így az európai polgárok és vállalkozások lehetőséget kapnak arra, hogy a digitális gazdaság nyújtotta előnyöket maradéktalanul kihasználhassák.

A GDPR megalkotóinak az is célja volt, hogy a kis- és középvállalkozások adminisztrációs terheit csökkentsék, továbbá törekedtek arra, hogy a jogszabály kövesse a „kockázatalapú megközelítést”[2].

Szakértői anyagok támasztják alá, hogy a GDPR jelentős változást hozott azáltal, hogy egy, az Európai Unió egész területén egységesen alkalmazandó adatvédelmi szabályozást ír elő, amely nemcsak a digitálisan tárolt személyes adatokra vonatkozik, hanem a papíralapúakra is, abban az esetben, ha azok valamilyen nyilvántartási rendszer részét képezik, vagy a későbbiek során képezni fogják. Az új szabályozás felváltotta a korábbi következetlen, mozaikszerű nemzeti jogszabályokat. Ezek szerint a vállalkozásoknak 28 jogszabály helyett csupán egyet kell alkalmazniuk, ami az adminisztratív terhek egyszerűsítése mellett a pénzügyi kiadások mértékét is csökkentheti.[3] Becslések szerint az új szabályok alkalmazása megközelítőleg 2,3 milliárd Euro hasznot is hozhat.[4]

---

1 95/46/EK rendeletet

2 Ha a GDPR előírja egy társaság számára az érintett jogait és szabadságait érintő kockázat felmérését, akkor a kockázat valószínűségét és súlyosságát objektív értékelés alapján, az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni.

3 A korábbi szabályozás alapján ugyanis az a cég, aki több tagállamban szeretett volna árukat eladni, vagy szolgáltatást nyújtani, mindenhol meg kellett felelnie a helyi adatvédelmi szabályozásnak és hatósági követelményeknek.

4 Az uniós adatvédelmi reform: Milyen előnyökkel jár a vállalkozások számára Európában? Európai Unió 2016, ISBN: 978-92-79-60207-8 http://ec.europa.eu/justice/data-protection/index_en.htm (Letöltés ideje: 2017. 12. 21.)

A financiális kiadások csökkenése mellett az új rendelet egyrészt nagyobb betekintést és jogokat biztosít a magánszemélyek részére adataik kezelésével kapcsolatban, másrészt a cégek ezirányú kötelezettségeit növeli, a mulasztásokat pedig az eddiginél jelentősebb pénzbüntetéssel sújtja.[5]

Fontos hangsúlyozni azt is, hogy a jogszabály nem csak az európai vállalatokat érinti, hatálya ugyanis kiterjed minden olyan EU-n kívüli cégre is, amely uniós polgárok adatait kezeli. Ezen felül az EU területén székhellyel nem rendelkező cégekre is vonatkozik a rendelet alkalmazása abban az esetben, ha szolgáltatásait az EU-ban kívánja nyújtani. Ez az előírás egyenlő versenyfeltételeket teremt minden vállalkozás számára.

Az új adatvédelmi rendelet biztosítja, hogy egyértelmű és érthető tájékoztatást kapjunk személyes adataink feldolgozása esetén. Mielőtt személyes adatainkat egy vállalkozás feldolgozza, hozzájárulásunkat félreérthetetlen módon kell megadni, továbbá a rendelet megerősíti a személyes adatok tárolásának megszüntetéséhez való jogot is.

Az új jogszabály szabadabbá és könnyebbé teszi a személyes adatainkhoz való hozzáférést, megkönnyíti számunkra, hogy megtudjuk, milyen személyes adatot tárolnak rólunk a vállalatok, közigazgatási hatóságok.

A nemzeti adatvédelmi felügyeleti hatóságok feladata, hogy ezeket a jogokat tudatosítsák, valamint iránymutatást adjanak arról, hogyan lehet velük a leghatékonyabb módon élni. Ezek az elvek hozzájárulnak ahhoz, hogy megnőjön bizalmunk személyes adataink kezelésével kapcsolatban, de segítségünkre lehetnek az online szolgáltatások biztonságos használatának erősítése vonatkozásában is.

Mire ösztönöz és milyen kötelezettségekkel jár a GDPR?

A GDPR – az adatbiztonság erősítése és az adatvédelemben érintett személyek védelme érdekében – meghatározza, hogy kötelezően ki kell nevezni adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő tevékenysége szélesebb adatkezelői körben zajlik, mint a 2011. évi CXII. törvény 24.§ (1) pontjában meghatározott belső adatvédelmi felelősé.

A változtatás célja az volt, hogy az új feladatkör független legyen, amely széles körű feladatokkal és nagyobb felelősséggel jár.

Az adatvédelmi tisztviselő kijelölése az alábbi esetekben kötelező[6]:

- Az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik;
- Az adatkezelő vagy adatfeldolgozó fő tevékenységei olyan adatkezelési műveletet foglalnak magukban, amelyek az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;

[5] https://ado.hu/rovatok/cegvilág/gdpr-mire-kell-figyelni (Letöltés ideje: 2017. 12. 21.)
[6] Az Európai Parlament és Tanács (EU) 2016/679 Rendelete 38. cikk

- Az adatkezelő vagy adatfeldolgozó fő tevékenységei[7] a személyes adatok különleges kategóriáinak és a büntetőjogi felelősség megállapítására vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Abban az esetben, ha az adatkezelő/adatfeldolgozó nem köteles adatvédelmi tisztviselőt kijelölni, ennek tényét célszerű dokumentálni.

Az adatvédelmi tisztviselő feladatköre[8] összetett, különösen az alábbi tevékenységekre terjed ki: tájékoztatási feladata van, ellenőrzi az adatvédelmi szabályoknak való megfelelést, szükség esetén szakmai tanácsot ad az adatvédelmi hatásvizsgálatra[9] vonatkozóan, valamint együttműködik, és tartja a kapcsolatot a felügyeleti hatóságokkal. Az adatvédelmi tisztviselő lehet az adatkezelő/adatfeldolgozó alkalmazottja, de szolgáltatási szerződés alapján külső személy vagy szervezet is elláthatja a feladatot. Az adatvédelmi tisztviselőnek rendelkeznie kell a feladatai ellátásához szükséges szakértelemmel. A szakértői ismeretek szükséges szintjét az adatkezelő/adatfeldolgozó által végzett adatkezelés, valamint az általuk kezelt személyes adatok tekintetében megkövetelt védelem alapján egyedileg kell megállapítani.

Fontos kiemelni, hogy az adatvédelmi tisztviselő feladatai ellátása körében nem utasítható, és speciális felmondási védelemben is részesül.

Az Adatvédelmi Rendelet alkalmazására történő felkészülés során az érintetteknek további iránymutatásokat kellett figyelembe venniük:

Az adatbiztonság magas szintű megteremtése érdekében fontos volt, hogy kiemelt figyelmet fordítsanak olyan fontos összetevőre, mint az adatvédelmi tudatosság erősítése. Ennek alapja az oktatás, amely során elsajátíthatók a jogszabályok is. Ezután be kellett iktatni az adatkezelés céljának és szempontrendszerének meghatározását, valamint az adatkezelés feltételeinek megteremtését oly módon, hogy az alkalmazók mindvégig biztosítani tudják az adatok kezelésének és feldolgozásának jogszerűségét és nyomonkövethetőségét.

A cikk elején már utaltam arra, hogy a rendelet biztosítja a polgároknak a személyes adataik feletti kontrolt, ennek értelmében jelentős tényező kell hogy legyen az érintett személy megfelelő tájékoztatása saját jogaira[10] vonatkozóan. Ennek értelmében az érintettnek tájékoztatást kell kapnia az adatkezelés tényéről, céljáról. Az információs önrendelkezési jog érvényesülésének szükségessége a természetes személyt az adatkezelés megszűnéséig megilleti. Hangsúlyoznom kell a természetes személynek azt a jogát is, hogy az – internet sajátosságaira való

---

7 Az a tevékenység, amely az adatkezelő vagy adatfeldolgozó céljainak eléréséhez szükséges.

8 Az Európai Parlament és Tanács (EU) 2016/679 Rendelete 39. cikk

9 Az adatvédelmi hatásvizsgálat tehát a rendelet betartásának elérésére és bizonyítására szolgáló eljárás. Célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, a kockázatok kezelésének elősegítése, kezelésükre szolgáló intézkedések meghatározásával.

10 Személyes adatokhoz való hozzáférés, azok helyesbítése, törlése, kezelésének korlátozása, profilalkotás és az automatizált adatkezelés elleni tiltakozás, adathordozhatósághoz való jog.

tekintettel – az adatokat azok minden elérési pontján törölheti, így megvalósul a tényleges joggyakorlat.

Amennyiben az érintett kéri, az adatkezelő köteles tájékoztatni az érintettet saját személyes adatával kapcsolatban, de ez online rendszeren keresztül is lehetséges.

Az információs önrendelkezési jog érvényesülése értelmében az érintett kérésére az adatkezelő késedelem nélkül köteles törölni személyes adatát, ha az érintett visszavonja hozzájárulását az adatkezeléshez.

A GDPR 8. végrehajtási pontjában a gyermekek személyes adatainak kezelésével kapcsolatos szabályok találhatók. Az új szabályok értelmében gyermekek személyes adatainak kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. Más esetben a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben lehetséges, ha a hozzájárulást a gyermek feletti szülői felügyeletet ellátó személy engedélyezte. A hozzájárulást illetően a tagállamok 13. életévnél nem alacsonyabb életkort is megállapíthatnak.

A GDPR szerint a személyes adat jogellenes kezelése vagy feldolgozása esetén bejelentési kötelezettség keletkezik. Az adatkezelő indokolatlan késedelem nélkül, legkésőbb 72 órával az incidens után megteszi a bejelentést a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Az új szabályozás szerint az adatkezelőnek az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell lefolytatni. Ha bebizonyosodik, hogy az adatkezelési műveletek lényegesen magas kockázattal járnak, az adatkezelést megelőzően a felügyeleti hatósággal konzultálni kell. A hatásvizsgálat során figyelemmel kell lenni az adatkezelés jellegére, hatókörére, körülményére és céljaira, valamint a kockázatok forrásaira. Magas kockázatú adatkezelési műveletek lehetnek: nagyszámú érintett; nagy mennyiségű személyes adat; kiszolgáltatott személyek, pl. gyermekek adatainak kezelése; profilalkotás; viselkedés vagy mozgás követése; különleges adatok kezelése. Valószínűsíthetően magas kockázat esetén a felügyeleti hatóság az adatkezelőnek/adatfeldolgozónak írásban tanácsot ad vagy gyakorolhatja hatáskörét. A szabályozás rendelkezik arról is, hogy mikor nem szükséges hatásvizsgálatot végezni.

A Rendelet 117. pontja rendelkezik arról, hogy a tagállamokban teljes függetlenséget élvező felügyeleti hatóságokat kell létrehozni. A 117 – 134. pontban leírtak szerint a hatóságok saját tagállamuk területén illetékesek az e rendelettel összhangban rájuk ruházott hatáskörök és feladatok gyakorlására, végzésére. A fő felügyeleti hatóság illetékes eljárni az adatkezelő, adatfeldolgozó által végzett, határokon átnyúló adatkezelés tekintetében. A fő felügyeleti hatóság az érintett felügyeleti hatóságokkal információcserét folytat, együttműködik, de jogosult arra is, hogy hatáskört ruházzon rá.

A GDPR gyakorlati alkalmazásával együtt járó kezdeti nehézségek

A GDPR hatályba lépése után hamar kiderült, hogy – a hosszú felkészülési időszak ellenére – a Rendelet előírásaiban rejlő bizonytalanság és a jogszabály körüli értelmezési nehézségek hatására még a felkészülést komolyan vevő cégek, vállalatok is számos nehézséggel szembesülnek munkájuk során. A Rendelet hatálya valójában mindenkit érint, hiszen valamilyen mértékben minden vállalkozás kezel személyes adatokat.

Amennyiben valamely cég, vállalkozás mégis azt gondolta, hogy rá nézve nem hatályos a Rendelet, ezért egyáltalán nem készült fel az alkalmazásra, ellenőrzés esetén komoly bírságot kaphat.

A Rendelkezés alkalmazása előtti felkészülési időszakban az érintettek közül sokan figyelmen kívül hagyták, hogy a rendelet betartása nem csupán egy vállalati részleg feladata. Az érintett vállalatok egy része a GDPR-ra való felkészülést mindössze a jogászokra és az informatikusokra bízta. A sikeres GDPR-megfelelőség azonban a rendszerszemléletben, az üzleti folyamatokban és a munkavállalók gondolkodásában rejlik. Ezek hiányában a felkészülésre fordított financiális befektetés értelmetlen lehet.

A felkészülés időszakát megnehezítette, hogy a GDPR kevés konkrét követelményt támaszt, sőt Magyarország egyik vezető adó- és üzleti társasága, a KPMG[11] vizsgálata szerint a Rendelet elvárta a cégektől, hogy maguk mérjék fel adatvédelmi kockázataikat, és határozzák meg adataik védelmének módját. Kérdés volt többek között, hogy mikortól kezel egy vállalkozás nagy mennyiségben adatot, hiszen egy vidéki kis üzlet számára néhány ezer fő is nagy vevőállományt jelent egy milliós nagyságrendű vásárlói körrel bíró európai webshoppal szemben. Ennek következményeként kellő információk, iránymutatások hiányában a vállalkozások kivárásra törekedtek, így a felkészülés sok esetben csúszással járt. A hazai példával ellentétben Franciaországban és Bajorországban születtek hatósági iránymutatások, Hollandia nyilvántartási mintát tett elérhetővé, másutt rendelkezésre álltak elfogadott magatartási kódexek. Ezek a viszonyítási pontok számunkra is elérhetők, de fontos figyelemmel lenni a magyar viszonyokra is.

Magyarországon az egyik legnagyobb kihívást a korlátozott tárolhatóság elvének való megfeleltetés jelenteti, hiszen emiatt tisztában kell lenniük a cégeknek hogy az egyes adatokat meddig tárolhatják és mikor kötelesek tárolni azokat. A cégek sok esetben az adatvagyon felmérése helyett jogi vagy informatikai „varázsszerekkel” akarják megoldani a tárolási és törlési idők problémáját.

A cégek, vállalkozások jelentős részét érinti a Rendelet beszállítói menedzsmenttel kapcsolatos szabályozása. Ez a szabályozás a felkészülési időszakban vihart kavart, mert a GDPR kimondja, hogy egy adatvédelmi incidens vagy hatósági vizsgálat esetén nem hivatkozhatunk arra, hogy az adatkezelési esemény nem nálunk, hanem a beszállítóknál történt. A GDPR ezzel az érintettek felelősségi körét saját határaikon túlra is kiterjesztette. Ez maga után vonja a már meglévő szerződések felülvizsgálatának elvégzését, szükség esetén kiegészítését.

[11] KPMG Hungária Kft. – könyvvizsgálati szolgáltatások
KPMG Tanácsadó Kft. – adó- és üzleti tanácsadó szolgáltatások

Jelen problémára a KPMG két megoldást javasol a cégeknek. Egyrészt lehetőségük van arra, hogy elfogadtassák a beszállítókkal azt, hogy maga a cég ellenőrizhesse a beszállítóknál zajló adatkezelés GDPR kompatibilitását, másrészt előírhatja a beszállító számára, hogy a megfelelőséget egy erre feljogosított független szervezet igazolja, tanúsítsa.

A GDPR hatályba lépése előtt is következetesen szankcionálták a helytelen adatkezelést: a Nemzeti Adatvédelmi és Információs Hatóság 2012-ben 18.600.000, 2013-ban 20.550.000 forint bírságot szabott ki.[12] A Rendelet bevezetése után az egyes országok adatvédelmi hatóságai révén kiszabható pénzbüntetés egységesen 10.000.000-20.000.000 euro között mozoghat. A tagállamok további közigazgatási és büntetőjogi szankciókat határozhatnak meg, például adatbázis jogellenes vásárlása esetén a jogsértés útján szerzett vagyon elvonását. A felkészülés tapasztalatai szerint ez a financiális szigorítás az érintettek jelentős hányadát nagyon megijesztette, és valószínűleg nem is ismerték fel azt, hogy ez a szigorú szabályozás miért szükséges. Véleményem szerint ennek az oka az, hogy a legtöbb GDPR felkészülést végző cég nincs tisztában az incidensek jelentőségével. A Rendelet szerint nem csak a bekövetkezett esemény minősül incidensnek, hanem már az is, amennyiben felvetődik annak a lehetősége, hogy személyes adatok sérülhetnek vagy elveszhetnek. A gyakorlatba átültetve: incidensnek minősül, ha elveszik egy személyes adatokat tartalmazó pendrive, de az is, amikor nem tudjuk a cég melyik dolgozójánál van. Az incidensek bekövetkezésének megelőzését akkor tudják a cégek legjobban teljesíteni, ha minden elvárható lépést megtesznek a kezelt adatok biztonsága érdekében.

A bírság kiszabása azért is kockázatos a vállalkozások számára, mert súlyos esetben elérheti a húszmillió eurot vagy a vállalkozás előző pénzügyi éve teljes világpiaci forgalmának 4%-át.

Egy 2018. 05. 29-én benyújtott, „Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényjogharmonizációs célú módosításáról” szóló törvényjavaslat szerint az Infotv. a következő 75/A. §-sal egészül ki:

„A Hatóság az általános adatvédelmi rendelet 83. cikk (2)-(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó – jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott – előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – az általános adatvédelmi rendelet 58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik.”

Ez alapján kiemelendő tehát, hogy a Hatóság a számára rendelkezésre álló hatásköröket az arányosság elvének figyelembevételével gyakorolja, amely azzal valósul meg, hogy a Hatóság a jogsértés első alkalmával elsősorban – az eset összes körülményére, így a jogsértés súlyára, annak ismétlődő jellegére valamint az érintetti kör nagyságára is figyelemmel – az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik. Az arányosság elvének alkalmazása nagymértékben

[12] www.securinfo.hu/termekek/piacok/adatvedelem/72gdpr (Letöltés ideje: 2018. 08. 27.)

segítheti a kis- és középvállalkozásokat az őket megterhelő financiális szankciók elkerülése érdekében.

A törvényjavaslat indoklása szerint a kezdeti időszakban a magas pénzbírság kiszabása elsősorban a multinacionális gazdasági társaságok felé irányul, mint például a Google vagy a Facebook.[13]

Összegzés

2018. május 25. óta az adatvédelmi jogszabályok minden uniós országban azonosak, ez azt jelenti, hogy a GDPR bevezetése által az EU tagállamainak adatvédelmét sikerült közös nevezőre hozni. A szabályozás közvetlenül alkalmazandó minden olyan szervezetnél, amely személyes adatot kezel. Ez közvetlen költségmegtakarítást és jogbiztonságot eredményez.

Az uniós rendelet hatályba lépése, az új irányelveknek való megfelelés jelentős átszervezési folyamatokat indított el, új szervezeti változásokat követelt, új beruházások, infrastruktúra kialakítások váltak szükségessé.

A jogszabály a korábbinál szigorúbb elvárásokat támaszt az adatokat kezelőkkel, felhasználókkal szemben. Ezzel együtt sokkal nagyobb ellenőrzési lehetőséget kapnak a felhasználók saját személyes adataik és azok felhasználása felett, mint amivel korábban rendelkeztek.

Nő a személyes adatokat feldolgozók felelőssége és elszámoltathatósága adatvédelmi kockázatértékelések, adatvédelmi tisztviselők, valamint a „beépített adatvédelem" és az „alapértelmezett adatvédelem" révén.

A GDPR bevezetése óta az egyes országok adatvédelmi hatóságai révén kiszabható pénzbüntetés egységesen 10.000.000 – 20.000.000 euro között mozoghat. A tagállamok további közigazgatási és büntetőjogi szankciókat határozhatnak meg, például adatbázis jogellenes vásárlása esetén a jogsértés útján szerzett vagyon elvonását.

Felhasznált irodalom:

- Dr. SZŰCS Ilona: Információbiztonság jogi aspektusból I.
- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete
- 2011. évi CXII. törvény
- Az Európai Parlament és Tanács (EU) 2016/679 Rendelete Letöltés ideje: 2017. 12. 21.
- https://jogaszvilag.hu/rovatok/cegvilag/munkahelyi-adakezeles-a-gdpr-alapjan (Letöltés ideje: 2017. 12. 21.)

[13] www.index.hu/tech/2018/5/29gdpr (Letöltés ideje: 2018. 06. 27.)

- http://naih.hu/felkeszueles-az-adatvedelmi- rendelet-alkalmazasara.html (Letöltés ideje: 2017. 12. 21.)
- Az Uniós Általános Adatvédelmi Rendelet bevezetésének hatásai a magyar adatvezérelt marketing szakma hétköznapjaira; DIMSZ Direkt és Interaktív Marketing Szövetség (Letöltés ideje: 2017. 12. 21.)
- http://ec.europa.eu/justice/data-protection/index_en.htm (Letöltés ideje: 2017. 12. 21.)
- https://ado.hu/rovatok/cegvilág/gdpr-mire-kell-figyelni (Letöltés ideje: 2017. 12. 21.)
- www.securinfo.hu/termekek/piacok/adatvedelem/72gdpr (Letöltés ideje: 2018. 08. 27.)
- www.index.hu/tech/2018/5/29gdpr 2018. 06. 27.
- Az uniós adatvédelmi reform: Milyen előnyökkel jár a vállalkozások számára Európában? Európai Unió 2016, ISBN: 978-92-79-60207-8 http://ec.europa.eu/justice/data-protection/index_en.htm (Letöltés ideje: 2017. 12. 21.)
- https://ado.hu/rovatok/cegvilág/gdpr-mire-kell-figyelni (Letöltés ideje: 2017. 12. 21.)
- Az Európai Parlament és Tanács (EU) 2016/679 Rendelete 38. cikk
- Az Európai Parlament és Tanács (EU) 2016/679 Rendelete 39. cikk
- www.securinfo.hu/termekek/piacok/adatvedelem/72gdpr (Letöltés ideje: 2018. 08. 27.)
- www.index.hu/tech/2018/5/29gdpr (Letöltés ideje: 2018. 06. 27.)

OTTI CSABA – DR. KOLNHOFER-DERECSKEI ANITA

AZ EMBEREK ELFOGADÁSI KÜSZÖBE A BIOMETRIKUS RENDSZEREK MEGBÍZHATÓSÁGÁVAL SZEMBEN[1]

Bevezetés

Ma már egyre több szakcikk és kutatás foglalkozik a biztonságmenedzsement kérdéskörével, Somroo és szerzőtársai[2] kiemelik a műszaki és menedzsment tudományok interdiszciplináris találkozását. Ezt a gyakorlat is megerősíti, hiszen elengedhetetlen, hogy a biztonságtechnikai kérdésekben döntéshozók (security personnel) felkészültek és járatosak legyenek a műszaki tudományokban is[3]. Kutatásunkban mi is ötvözzük a mérnöki tudományokat a társadalomtudománnyal, és rámutatunk arra, hogy a mérnökök számára az egyén emberi mivoltának pontos ismerete sosem lesz elhanyagolható.

Az általunk vizsgált téma relevanciáját a most divatos GDPR kérdésköre is adhatná, de most nem az adatkezelés jogi szabályozásával foglalkozunk, hanem a biztonságmenedzsment és biztonságtechnika egy másik szegmensével, a biometrikus beléptető rendszerekkel. A biztonságmenedzsment egyik jelentős területe az IT biztonság mellett a fizikai biztonság megteremtése, melynek általános részei: mechanikai védelem, elektronikai védelem és élőerős védelem. A biztonság megteremtésének egyik alapvető feladata, hogy az adott objektumhoz, személyhez vagy információhoz történő hozzáférést csak az arra jogosultak tehessék meg. A biztonságtechnikai rendszerek jelentős része erre a feladatra fókuszál. Az automatikus személyazonosítás (beléptető rendszerek) területén három alaptechnológia létezik: tudás alapú (PIN kód, jelszó) birtok alapú (kártya, telefon) vagy biometrikus azonosítású (valamely testi jellemző)[4].

Egy ilyen rendszer kiválasztása és bevezetése a felsővezetői döntés hatásköre, ahol a döntéselőkészítést mérnökök végzik, de a legtöbb esetben nekik sem állnak rendelkezésre az erőforrások, hogy hitelesen leteszteljék a szóba jöhető technológiákat. Cikkünk célja, hogy az alapfogalmak megismerésével közelebb kerüljünk ehhez a témakörhöz, ugyanakkor rá szeretnénk világítani arra, hogy a felhasználók sokkal elfogadóbbak a hibákat tekintve, és ez az elfogadási küszöb nagyságrendekkel eltér a rendszerek műszaki hibamutatóitól.

1 A publikáció az Emberi Erőforrások Minisztériuma ÚNKP-ÚNKP-18-3-III-OE-106. kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

2 SOOMRO, Zahoor Ahmed – SHAH, Mahmood Hussain – AHMED, Javed Information security management needs more holistic approach, A. International Journal of Information Management, 2016, pp. 215-225.

3 PELTIER, Thomas R.: Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management, CRC Press, 2016

4 OTTI Csaba: Comparison of biometric identification methods. 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara, 2016

Az automatizált, elektronikus biometrikus személyazonosítás hatalmas fejlődésen ment keresztül az elmúlt ötven évben. A rendészeti szerveknek egyre nagyobb az igénye arra, hogy személyeket hitelesen és gyorsan, gyakorlatilag bárhol képesek legyenek azonosítani. Ezzel párhuzamosan az élet minden területén egyre inkább szükséges a felhasználók, belépők azonosítása, a hozzáférés hitelesítése. Másrészről világosan látszik, hogy a felhasználói elfogadottság az egyes technológiák vagy berendezések irányában döntő szerepet játszik ezek sikerességében, mindennapos használhatóságában[5].

Kutatásaink során azonosítottuk azokat az elsősorban civil biometrikus alkalmazásokat, ahol a biometrikus azonosítás kritikus működésű, ezek a nagy munkavállalói létszámú vállalatoknál használt beléptető és munkaidő-nyilvántartó rendszerek[6]. A kritikusságot az adja, hogy a nagy létszám miatt gyorsnak és alacsony hibás elutasítási (FRR – False Rejection Rate) értékűnek kell lennie a rendszernek.

Magyarországon az elmúlt 20 évben megvizsgált mintegy 100 biometrikus rendszer bevezetés jelentős része sikertelen volt, és napjainkban is csak a "szerencse" dönti el, hogy sikeres lesz-e. Ezt a jelenséget elemezve jutottunk el az ABI-ban (Alkalmazott Biometria Intézet) 2010-ben biometrikus eszközök teszteléséhez. A tesztekkel bármely gyártó bármely eszközét vizsgálva arra jutottunk, hogy a megadott FRR adatok több nagyságrenddel eltérnek a valós értékektől. Ennek elsődleges oka, hogy a gyártók algoritmikus vagy más néven technológiai tesztek eredményeit adják meg, és nem számolnak a felhasználókkal, a telepítési és környezeti körülményekkel.

Ekkor már az merült fel bennünk kérdésként, hogy egyáltalán hogyan lehetséges, hogy léteznek sikeres biometrikus projektek? Másképpen megközelítve, el lehet-e dönteni egy biometrikus eszközről egy tender során, hogy az jól fog működni vagy sem.

Ezért a mindennapi felhasználók felé fordultunk, hogy ők hogyan látják ezt a kérdést. A hipotézisünk az volt, hogy az emberek legalább 2-3 nagyságrenddel nagyobb FRR-t hibás elutasítási arányt is még használhatónak fogadnak el. A kutatás előző szakaszaiban lefolytatott szakértői és fókuszcsoportos kutatásokban kidolgoztuk azt, a kérdéssort, amivel lefolytattuk a kvantitatív kutatást[7].

Jelen tanulmány 653 válasz alapján elemzi a feltett kérdéseket és összegzi az eredményeket.

---

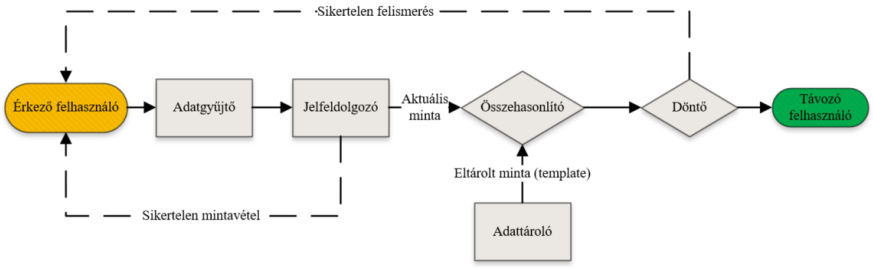
5 DILLON, Andrew – MORRIS, Michael: User acceptance of new information technology: theories and models. Annual Review of Information Science and Technology, 1996, 31. évf., pp. 3-32.

6 OTTI, i.m.

7 OTTI Csaba: Why does it fail to operate? In Thinking Together: The economy in practice, Budapest, 2017, Óbudai Egyetem, pp. 45–66.

A biometrikus rendszerek jellemzése

A vonatkozó ISO szabvány (ISO/IEC, ISO/IEC 2006) és Shimon Modi Biometrics in Identity Management: Concepts to Applications cikke alapján[8] a biometrikus berendezések alapvetően mintafelismerő rendszerek, általánosságban az 1. ábrán látható alrendszerekből állnak össze:



1 ábra: Általános biometrikus eszköz alrendszerei
(saját szerkesztés)

Az adatgyűjtő alrendszer felelős a felhasználó biometrikus mintájának levételéért. A rendszerbe ezen a ponton bekerült hibák végigfutnak a teljes azonosítási folyamaton. A jelfeldolgozó alrendszer feladata a mintákból kinyerni azokat a tulajdonságokat, amelyek egyedivé teszik azt. Az adattároló tárolja a levett és kódolt biometrikus adatokat a későbbi összehasonlításhoz. Ezeket az adatokat a biometria területén sablonnak is nevezik. A tárolás lehet központi (egy számítógépen vagy szerveren), illetve lokalizált (pl. smart cardon vagy egyéni adathordozó eszközön). 2018. május 25. után az EU 2016/679-es rendeletével gyakorlatilag betiltja a felhasználók biometrikus adatának központi tárolását. Az összehasonlító alrendszer összehasonlít két mintát és létrehoz egy hasonlósági pontszámot. Ez a pontszám annak bizonyosságát mutatja meg, hogy a tárolt sablon és a levett minta egy és ugyanazon személytől származik. A biometrikus azonosító rendszerek mindig valószínűség alapúak, így sosem jöhet létre 100%-os egyezés. Ezzel szemben például egy kriptografikus vagy jelszó alapú rendszernél mindig 100%-os egyezés szükséges a sikeres azonosításhoz. Mivel az ember és a szenzor találkozása sosem lehet kétszer pontosan ugyanolyan, ezért a rendszer egy egyszerű „igen” vagy „nem” válasz helyett egy hasonlósági pontszámot generál. A döntéshozó alrendszer összeveti a generált hasonlósági pontszámot egy előre meghatározott határértékkel, hogy eldöntse az azonosítás sikerességét vagy sikertelenségét.

A hibák

Az ellenőrzési és azonosítási hibák vagy megfeleltetési (téves egyezési ill. téves nem egyezési hibák), vagy mintavételi hibákra (sikertelen mintavétel, sikertelen rendszerbe való felvétel) vezethetőek vissza. Az, hogy ezek az alapvető hibák miként vezetnek döntési hibához, több tényezőn múlik, mint például az előírt

[8] SHIMON, Modi K: Biometrics in Identity Management: Concepts to Applications, Nordwood, Artech House, 2011

összehasonlítások számán; a döntési policyn, vagy éppen azon, hogy pozitív vagy negatív-e az azonosítás[9].

Egy biometrikus azonosító rendszer két hibatípust képes generálni.

- Két különböző személy biometrikus mintájának téves mérését és egyezőként azonosítani (Téves megfeleltetés – false match, szakirodalmi mutatószáma False Match Rate – FMR vagy False Acceptance Rate – FAR).
- Ugyanattól a személytől két mérést különböző személyként azonosítani (Téves meg nem feleltetés – false nonmatch, szakirodalmi mutatószáma FNMR – False Non Match Rate vagy FRR – False Rejection Rate)

Minden rendszerben létezik egy tradeoff görbe a hibás egyezési ráta (FMR – False Match Rate) és a hibás nem-egyezési ráta (FNMR – False Non Match Rate) között. Ha úgy konfigurálják a rendszert, hogy kevésbé legyen érzékeny a zavaró tényezőkre és jobban fogadja el a felhasználók mintáit, akkor az FMR nő meg, ha biztonságosabb beállításokat hoznak létre, akkor pedig az FNMR. A biometrikus rendszerek teljesítményének ábrázolására általánosan ROC (Receiver Operating Characteristic) és DET (Detection Error Tradeoff) görbéket használnak.

Mutatószámok

A szakirodalomban nincs (vagy több is létezik) egységesen használt és elfogadott definíciója a biometrikus rendszereket jellemző mutatószámoknak, ezért ebben a fejezetben ismertetjük az általunk használt elnevezéseket. Elsősorban a 2006-os és 2012-es ISO/IEC 19795 szabványt használjuk fel, ahol ettől eltérünk ott azt jelezzük és megindokoljuk.[10] Az alábbiakban dióhéjban összefoglaljuk a biometrikus beléptető rendszerek műszaki paramétereit jellemző ismérveket.

1. **Sikertelen regisztráció arány - Failure To Enroll rate (FTE)**
   Ez a mutató azt jelzi, hogy egy rendszerbe milyen valószínűséggel nem lehet beregisztrálni a felhasználókat. Általában a felhasználó biometrikus mintája alkalmatlan a feladatra, de ide tartoznak azok az esetek is, amikor valamilyen más ok miatt sikertelen a regisztráció, például rosszul tette rá a szenzorra a mintát. Az arány a regisztrálandó populációra és az adott berendezésre ad előjelzést.
2. **Sikertelen mintabeviteli arány – Failure To Acquire rate (FTA)**
   A sikertelen mintabevitel azt jelenti, hogy az eszköz valamilyen okból képtelen levenni a mintát és abból előállítani azt a kódot, amit összehasonlítana az adatbázisával. Az ebből képzett arány pedig az összes sikeres mintabevitelre vetíti a sikertelen eseteket.

---

9 JAIN, Anil. K. – FELLOW, ArindamGhosh. R.. – PRABHAKAR, Salil: An Introduction to Biometric Recognition. EEE Transactions on Circuits and Systems for Video Technology, 1. évf. 14. sz., 2004, pp. 4-20.

10 ISO/IEC. (2006, április). ISO/IEC 19795-1 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. 2016, Svájc. és ISO/IEC. (2012). ISO/IEC 19795-6:2012(E). Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation. Svájc, 2012

3. **Téves meg nem feleltetés – False None-Match Rate (FNMR)**
   Az FNMR jelenti azt a várható értéket, hogy két minta ugyanattól a személytől hibásan különbözőnek lett felismerve az algoritmus által.

4. **Téves megfeleltetés – False Match Rate (FMR)**
   Az FMR jelenti azt a várható értéket, hogy két különböző minta hibásan egyezőnek lett felismerve az algoritmus által.

5. **Téves elutasítási arány - False Reject Rate (FRR)**
   Az FRR-t számos szakirodalom alkalmazza az FNMR szinonímájaként, azonban mi a céljainknak jobban megfelelő és a szabványban is így definált verziót alkalmazzuk:

   $$FRR = FTA + FNMR * (1 - FTA)$$

   Mi ezt a mutatót választottuk, mert ez felel meg leginkább a céljainknak, ennek értelmezése áll a legközelebb az általunk felmérni kívánt jelenséghez.

6. **Téves elfogadási arány - False Accept Rate (FAR)**
   A téves elfogadási arány megmutatja annak a valószínűségét, hogy egy – szándékosságot mellőző – jogosulatlan személy mintáját tévesen elfogadja a rendszer.
   Kiszámítására alkalmazható képlet:

   $$FAR = FMR * (1 - FTA)$$

7. **Általánosított téves elfogadási és elutasítási arány – Generalized False Reject Rate (GFRR) – Generalized False Accept Rate (GFAR)**
   A különböző biometrikus rendszerek eltérő Sikertelen Regisztráció Aránnyal (FTE) rendelkeznek, ezek az esetek azonban kiesnek az előző mutatószámokból, mivel jellemzően a továbbiakban nem vizsgálják azokat. Ezért került bevezetésre az általánosított téves elfogadási és elutasítási arány, amely mutatók egyesítik a regisztrációs, a mintavételi és az algoritmikus hibákat is.
   A GFRR és GFAR kiszámítására alkalmazható képletek:

   $$GFRR = FTE + (1 - FTE) * FTA + (1 - FTE) * (1 - FTA) * FMR$$

   $$GFAR = (1 - FTE) * (1 - FTA) * FMR$$

A hibás elutasítási arány jelentősége a gyakorlatban

A False Rejection Rate – Hibás elutasítási arány látszólag másodlagos mutatószám a biometrikus azonosítás területén. Ez azért történhet meg, mert a FAR – téves elfogadási arány, sokkal inkább „félelmetes” a biztonság tervezésénél – be tud menni olyan személy a védett területre, aki nem jogosult (impostor). Ez számos alkalmazásban igaz is, azonban a fizikai biztonság területén, tömegtartózkodású objektumokban (beléptetés és munkaidő nyilvántartás, több, mint 300 fő), Magyarországon az elmúlt 20 évben nem találkoztunk olyan alkalmazással, ahol ez a tényező dominált volna. Ez egyszerűen belátható, ha matematikai kockázatelemzési módszereket használunk és a felhasználók beléptetésének ideje és sikeressége jelentős szempont az alkalmazásnál[11].

[11] MICHELBERGER Pál – HORVÁTH, Zs.: Security aspects of process resource planning. Polish Journal of Management Studie, 2017, pp. 142-153.

Az FRR becslése, mérése és megadása az általunk feldolgozott szakirodalom alapján szinte kivétel nélkül technológiai eredményekre szorítkozott – ami nem meglepő, mert ez az egyetlen olyan teszttípus, amelyik jól kontrollálható, nagy tömegű mintán futtatható és egyértelmű sorrendet képes felállítani az algoritmusok között. A gyártók ezeket az FRR értékeket tüntetik fel az eszközeik adatlapján, általában 0,00001%-0,01% tartományban.

Az ABI-ban elvégzett forgatókönyvi, valamint éles körülmények közötti tesztek eredményeit megvizsgálva azt találtuk, hogy a valóságban a felhasználók az 1-70% tartományban találkoznak a hibás elutasításokkal. Ez azt jelenti, hogy legalább 2, de akár 6 (!) nagyságrend különbség is lehet az adatlapi ígéret és a valós eredmények között. Mivel az adatlapi értékek a gyakorlatban mérhetetlenek, ez két dolgot eredményez egy biztonsági beruházás döntésénél:

- Minden gyártó eszköze megfelel a kiírásnak.
- Eldönthetetlen, hogy melyik rendszer lesz a megfelelő az adott feladatra.

Emiatt a döntési pontok eltolódnak és más szempontok kerülnek előtérbe, mint például az ár.

Forgatókönyvi FRR mérések

A vonatkozó biometrikus rendszerek teszteléséről szóló ISO szabványok és saját módszertani fejlesztések alapján a forgatókönyvi teszteknél olyan körülményeket alakítottunk ki, amelyekkel a felhasználók a valós életben is találkozni fognak. Ilyen például egy arcfelismerő berendezés fényviszony függése, amely tesztelésével pontosan megmondható, hogy egy kültérre telepített eszköz a napfény megvilágításával a különböző napszakokban hogyan fog viselkedni.[12]

Ahogy azt vártuk is, a körülmények ideálistól való eltérésekor az FRR értékek romlanak. Az egyes eszközök között az tesz különbséget és dönti el a használhatóságot, hogy milyen mértékben és milyen gyorsan romlanak el az eredmények.

A valós körülményeket minél jobban megközelítő eljárások kerültek kidolgozásra úgy, hogy a mérések feltételei, körülményei pontosan dokumentáltak legyenek a megismételhetőség miatt:

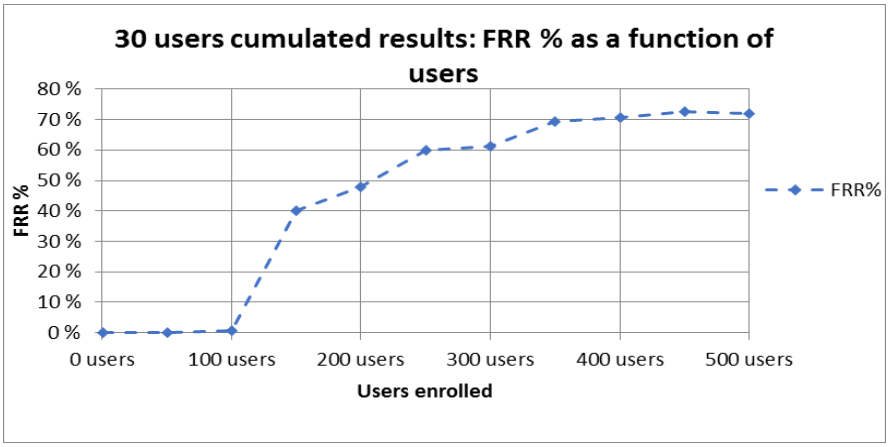
- Pozícionálási érzékenység: a tökéletesen pozícionált minta elforgatásra és eltolásra kerül, és mérjük az FRR változását.
- Áteresztőképesség mérése a regisztrált felhasználók és minták függvényében.
- FRR mérése a regisztrált felhasználók és minták függvényében.
- Minta szennyezése: például egy nedves ujj.
- Minta torzítása: például egy felsértett ujj vagy gyűrű.
- Környezeti változások hatásai: megvilágítás, hőmérséklet, páratartalom.

[12] ISO/IEC: ISO/IEC 19795-1

Az FRR mérések statisztikai hátterének elemzésére kiváló összefoglalást ad Hanka[13] publikációja. Ebben bebizonyítja és kiterjeszti a biometrikus ujjnyomat-azonosító rendszerekre Doddington 30-as szabályát, mely szerint: *„90%-os konfidencia szint esetén, legalább 30 hibát kell észlelnünk, hogy a keresett p valószínűség a tapasztalat alapján számított relatív gyakoriság ± 30%-os környezetébe essen."* Jelen esetben a *p* valószínűség az FRR értéke és az elv értelmében adott FRR szint elfogadásához 30 hibát kell mérnünk. Ez azt jelenti, hogy egy átlagos biometrikus eszköz FRR=0,01% méréséhez **300.000** eseményt, azaz mérést kellene elvégeznünk. Ezt gyakorlatilag lehetetlen kivitelezni.

A valóságban azért mégis értelmezhető eredményeket kaptunk, erre a legjobb példa egy ujjnyomat azonosító berendezés FRR függése a regisztrált minták számától.

A mérési metodika szerint a névleges felhasználói kapacitást (500 fő) 50 fős lépésközökkel töltöttünk fel és minden mérési pontban 300 mérést végeztünk el. Az eredmények a következő ábrán láthatóak.



2. ábra: Arcfelismerő eszköz forgatókönyvi tesztjének eredménye. FRR% a regisztrált létszám függvényében
(saját szerkesztés)

A kutatás

Ezen kutatásunk célja felmérni, hogy az emberek mikor és mennyire éreznek használhatónak egy biometrikus beléptetőrendszert annak függvényében, hogy hányszor sikertelen az áthaladási kísérletük. A „Why does it fail to operate?"[14] publikációban fókuszcsoportos felméréssel meghatároztuk az emberek spontán válaszait, tapasztalatait és érzéseit. Az elemzés alapján arra jutottunk, hogy szinte még egy homogén csoportban (Óbudai Egyetem, Keleti Kar, másoddiplomás

[13] HANKA László: A Doddington-féle 30-as szabály, biometrikus rendszerek megbízhatóságának statisztikai elemzése. Tavaszi Biztonságtechnikai Szimpózium, 2013, Budapest, Óbudai Egyetem

[14] OTTI i. m.

osztály) sincs azonos fogalmi kör. Ezt a tapasztalataink is teljes mértékben alátámasztják.

Ezután nagyon sokat gondolkodtunk azon, hogyan lehetne egy olyan általános modellt és megfogalmazást kitalálni, amit várhatóan mindenki megért, ugyanazt gondolja róla, érdemben tud is rá válaszolni, és a kutatási kérdéseinkre is választ ad. Először a biometria került ki a meghatározásból, később a beléptető rendszer is. Végül addig egyszerűsítettük, hogy egy ajtón való áthaladásról kérdeztünk, amely ajtó néha megszorul, és ezért nem nyílik ki. Ennél a példánál analóg módon lehet értelmezni a sikertelen belépések számát, azonban nem triviális, hogy melyik értékeknek felel meg. Az előző fejezetben tárgyalt mutatószámok közül az FRR értéket választottuk, mivel az tartalmazza az algoritmikus FMR, a sikertelen mintabeviteli hibákat is.

Kutatási kérdés és hipotézisek

Továbbiakban a fentebb leírt mutatók közül az FRR-rel dolgozunk tovább. Az előkészítési szakaszban többször viccesen neveztük a kutatásunk tárgyát az „emberi FRR”-nek. Ez alatt azt értettük, hogy vajon mi az a hibamutató, melyet a hétköznapi felhasználó érzékel, és valójában mennyire érzékeny a hibákra a felhasználó. Azaz hol találkozik a rendszer és az egyén hibamutatója? Kutatásaink során megfogalmazott hipotéziseink a következőek:

H1: A fennakadás gyakorisága és a rendszer megítélt használhatósága között összefüggés van.
H2: Az emberek elfogadási küszöbe több nagyságrenddel magasabb, mint a gyártók által az eszközre megadott FRR – téves elutasítási értéke.

Amennyiben sikerül igazolnunk a hipotéziseket, úgy a forgatókönyvi tesztek alapján kapott értékek egyrészt a valóságban statisztikailag is validálhatók, másrészt ténylegesen prediktálni lehet a rendszer használhatóságát az adott alkalmazásban.

A kérdés szövege így hangzott:
„Képzelje el, hogy heti 5 napon keresztül, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Ez az ajtó általában jól működik, ám ……. (megakadási gyakoriság) egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?”

A megakadás gyakoriságát az áthaladások számának függvényében határoztuk meg, ehhez a következő egységekkel dolgoztunk:

- naponta egyszer (leggyakoribb)
- hetente egyszer
- havonta egyszer
- évente egyszer

Amennyiben feltételezzük, hogy a válaszadó minden hétköznap legalább négyszer áthalad a kérdezett kapun (2 belépés és 2 kilépés), akkor havi átlagos 20 munkanappal számolva az évente 960 áthaladást jelent, vagyis a fennakadások relatív gyakorisága évente:

- napi egyszeri fennakadásnál 25%
- heti egyszeri fennakadásnál 5,415%

- havi egyszeri fennakadásnál 1,25%
- éves egyszeri fennakadásnál 0,104%

A megítélt használhatóságot négy fokozatú szemantikus differenciál skálán mértük a következő fokozatokat alkalmazva:

- használhatatlan – 1-es érték
- kevésbé használható – 2-es érték
- használható – 3-as érték
- tökéletesen használható – 4-es érték

Mindkét ismérv ordinális skálán mért adatokat jelent. Az elemzés során az alábbi statisztikai eljárásokat alkalmaztuk: leíró statisztika, intervallumbecslés (90%-os konfidencia intervallummal, mely értéket a biometrikus rendszerek értékelésénél használatos Doddington szabály indokol), kereszttábla elemzések (α=0,05 szignifikancia teszttel) és nemparametrikus hipotézis próbák (ugyancsak p = 0,95), valamint regresszió analízis.

Alkalmazott módszertan

Az adatok felvétele 2017 márciusa és áprilisa között történt az Óbudai Egyetem hallgatóinak (446 fő, a kitöltők 60,8%-a) és a MENSA HungarIQ tagjainak (197 fő, a kitöltők 26,8%-a), valamint egyéb egyetemi hallgatók körében (91 fő, a kitöltők 12,4%-a) körében. A célcsoportválasztásunkat két dolog indokolta, egyfelől az Óbudai Egyetem Campusain a hallgatók már találkoznak és naponta használnak beléptető kapukat, másfelől ők képezik majd a munkaerőpiac szerves részét, ahol a tapasztalataink alapján a vállalatok döntő többségénél, a nagyvállalatok mindegyikénél találkoznak ilyen beléptető rendszerekkel. Az Óbudai Egyetem hallgatói közül 390 fő a Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar hallgatója, ők nem csak találkoznak ilyen rendszerekkel, de tanulmányaikban is megjelennek. A kitöltők egy része dolgozik is (497 fő), jellemzően azokon a területeken ahol találkoznak ilyen rendszerekkel. A kutatás során kérdőívet alkalmaztunk, melynek szövege egyfelől a korábbi kutatásokon alapult[15], másfelől szakirodalmi feldolgozásaink adták. Mivel a kutatási alanyoknak nem valós, hanem egy elképzelt, hipotetikus helyzetben kellett az ajtón való fennakadás problémáját megítélniük, így a kérdőívet több alkalommal teszteltük.

Minta elemzése

Az adatok tisztítása után n=734 kitöltő válaszaival dolgoztunk, ezt az elemszámot további 653-ra csökkentettük, ami azon válaszadókat fedi le, akik minden válaszra feleltek. A válaszadók megoszlása a következőképpen alakult.

Nemek szerinti megoszlásban a kitöltők 74,4%-a (486 fő) férfi és 25,6%-a (167 fő) nő, amit az Óbudai Egyetem profilja indokol.

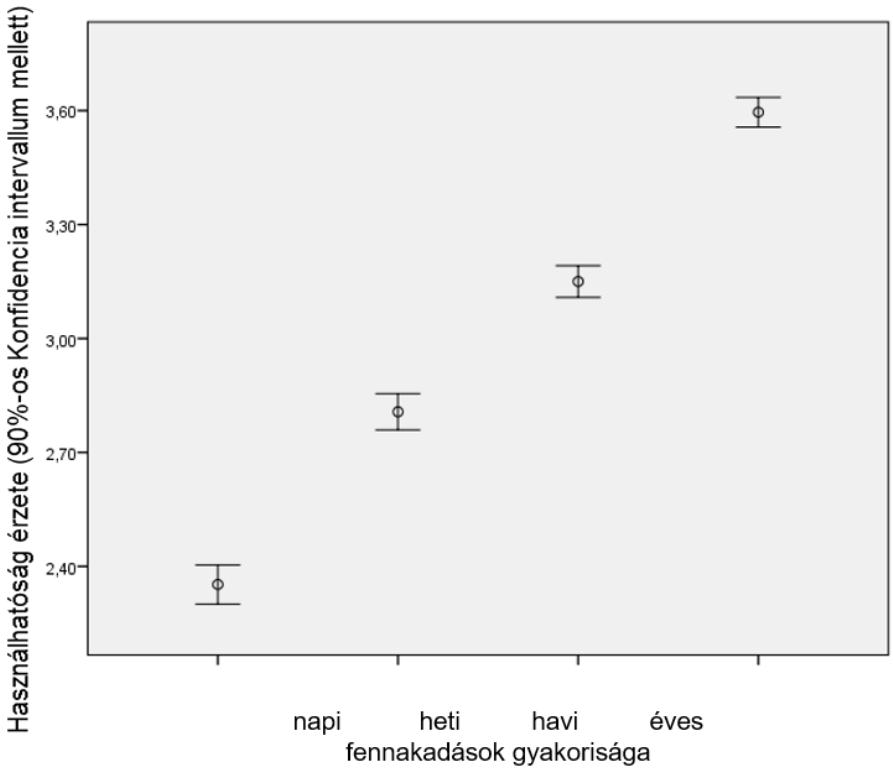
Mivel a mintaválasztás nem véletlen, önkényes kiválasztáson alapult, célunk a minta elemszámának növelése volt, így a mintánk habár nagy elemszámú, de nem

[15] Otti Csaba: Comparison of biometric identification methods. 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI).

tekinthető minden szempontból reprezentatívnak. Feltételezhetően igazodik a megjelölt populációhoz, vagyis a beléptető kapukat használók sokaságához, külön súlyokat nem használtunk. A kapott válaszok kitűnő iránymutatást adnak, hiszen ilyen magas kitöltői számnál a centrális határeloszlás által a normális eloszlással számolhatunk. Az egyes vizsgált ismérvek esetén normalitás (illeszkedés) vizsgálat is történt.

Eredmények

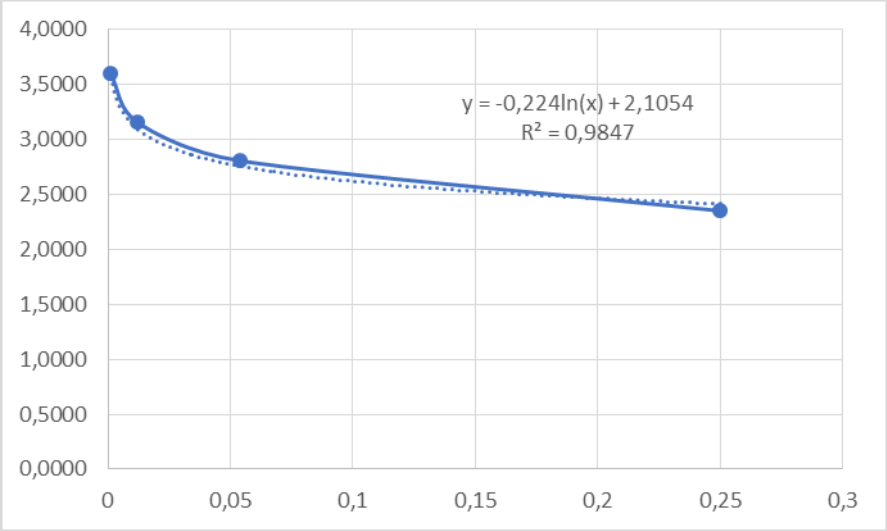
A fennakadások gyakorisága és a használhatóság megítélésében szembetűnő (szignifikáns sig.p < 0.05) összefüggés van. A fennakadások gyakoriságának csökkenésével nő az elégedettség. Az összefüggés számszerűsíthető értéke Pearson féle korrelációval R = 0.543, közepesen erős összefüggést mutat.



3. ábra: A válaszadók átlagos elégedettsége a fennakadások gyakoriságának függvényében 90%-os konfidencia intervallum mellett n=635
(saját szerkesztés)

Amennyiben az időegységet nem ordinális, hanem arányskálán vizsgáljuk, azaz a fennakadások gyakoriságát a fentebb leírt százalékos (relatív) megoszlásban vizsgáljuk, az érték nagyon hasonló lesz (R = - 0,479, a negatív értéket indokolja, hogy ahogyan csökken a fennakadások gyakorisága, úgy nő a felhasználó elégedettsége). Ez a közepesen erős szignifikáns együttjárás lehetőséget biztosít

arra, hogy regressziós függvényt illesszünk az adatokra. Az illesztés során már a fennakadások gyakoriságát az időegység százalékában vizsgáltuk. A legjobb illeszkedés a logaritmikus függvény esetén mutatkozik, melyet a következő 4. ábra szemléltet. A konstans értéke itt 2,1054, vagyis semleges a beállítódás az ajtó fennakadására, amely a fennakadás gyakoriságának a növekedésével csökkenti az eszköz használhatóságának az értékét, ebben az esetben a fennakadás gyakoriságának egy egy százalékos (itt a 960 éves áthaladási alkalomból, napi négyszeri áthaladásnál vett egy százaléka) emelkedése a felhasználó 0,224 egységnyi használhatósági érzet csökkenéssel jár (a fentebb leírt 4 fokozatú skálán tekintve).



4. ábra: A válaszadó átlagos elégedettségi szintjére illesztett regressziós függvény a fennakadások gyakoriságának függvényében n=635 (X tengelyen: fennakadás éves relatív gyakorisága, Y tengelyen: használhatósági/elégedettségi szint mértéke)
(saját szerkesztés)

Ez a vizsgálat igazolta a H1 hipotézisünket, mely szerint a fennakadás gyakorisága és a rendszer megítélt használhatósága között összefüggés van. Mi több, ez az összefüggés oly mértékű, mely alapján logaritmikus regressziós függvényt is illesztettünk rá. Azonban vissza kell térnünk arra, hogy a magyarázó erő (R négyzete) 0,295, azaz a fennakadások gyakorisága csak közel 30%-ban magyarázza a felhasználó megelégedettségét. Így adódik a kérdés, hogy még mi lehet hatással a felhasználó megelégedettségére. A vizsgálat során a demográfiai jellemzők mellett megkérdeztük a felhasználókat a munkahelyi megelégedettségükről is, ezek használatának az oka, hogy a kitöltők célzottan nem egymásutáni sorrendben kapták az általunk kutatott problémát, így az egyes válaszaik közé épített kérdések csökkentették a kitöltés során a telítődést, fenntartották a kitöltő érdeklődését.

- Hogyan érzi magát most?
- Mennyire elégedett a munkájához/tanulmányaihoz kapott információkkal?
- Mennyire ajánlaná másnak a jelenlegi munkahelyét/iskoláját?

A válaszokat itt is szemantikus differenciál skálán adhatták meg a válaszadók. Habár érdekes lehet, de a jelen cikkünkben nem térünk ki ezen kérdésekre adott válaszok egyenkénti elemzésére, csak azokat az együttjárásokat mutatjuk be, ahol a felhasználó aznapi általános közérzete és munkája iránti érzelmei hatással vannak az általunk vizsgált használhatósági értékre. Az összehasonlítás során az általános eszköz megelégedettségi szintet néztük, ahol szignifikáns összefüggéseket találtunk (sig. $p < 0,05$), azok a következő jellemzők voltak: (1) aki jobban érezte magát, vagyis magasabb értéket jelölt meg ezen a skálán az általánosan az eszközt is jobban használhatónak értékelte (Cramer értéke 0,179) (2) minél jobban úgy érzi, hogy több információt kap a válaszadó, annál elégedettebb az eszközzel is (Cramer értéke 0,197) (3) ez esetben a kapcsolat iránya nem került azonosításra (az ok-okozati összefüggés), de szignifikáns összefüggés mutatkozott az eszköz elégedettség és az ajánlás mértékével (Cramer értéke 0,161). A legerősebb összefüggés az információ esetén mutatkozik, egy másik kérdésben az előreláthatóság arányát jelölték meg a legtöbben legfőbb munkahelyi stresszforrásként. Ez rámutat arra, hogy az oktatás, megfelelő tájékoztatás és információ átadás csökkenti a bizonytalanságot és ezáltal javítja az eszköz használata iránti érzelmeket, annak elfogadását.

Látható, hogy mindenhol szignifikáns, de nagyon gyenge összefüggés mutatható ki, ezért a fenti modellünk magyarázó erejét csak gyengítenék ezen faktorok egy többtényezős regressziós modell alkalmazásának esetén, ezért elfogadjuk a kéttényezős modellt.

A H2 hipotézis szerint a felhasználók elfogadási küszöbe több nagyságrenddel magasabb, mint az adatlapokon általában megadásra kerülő hibás elutasítási arány (FRR = 0,01%). Ahogyan látható a 4. ábrán a 3.00 „Használható” értékhez körülbelül 3%-os FRR tartozik. Ezzel igazoltuk a H2 hipotézisünket is.

Konklúziók és összegzés

Peltier[16] rendszerezi azokat a jellemzőket, melyek a biztonságot segítendő rendszerek bevezetése előtt megfontolandóak.[17] Mi ezek közül a felhasználók véleményére fókuszáltunk, összevetve az általuk adott elfogadást (jóság mutatót) a rendszerek műszaki paramétereivel. Ugyanis a kutatásunk alanya a végső felhasználó, akit nem műszaki paraméterein keresztül, hanem társadalomtudományi módszerekkel hipotetikus helyzetben elképzelt szituációkra adott introspektív válaszai által tesztelünk.

Ebben a tanulmányban a mérnöki-menedzsmenti szemlélet kettősét, ennek egyik szegmensét a biometrikus rendszerek vizsgálatát vettük górcső alá. Egy ilyen rendszer bevezetése előtt számtalan szakmai adattal szembesül a döntéshozó. Mi elsőként bemutatjuk a biometrikus rendszereket a mérnöki mérőszámokon és fogalmakon keresztül, hiszen a döntéshozó a rendszer hibáit ezen mutatókon keresztül ismeri meg. Ugyanakkor kutatásunk során rávilágítunk arra, hogy a végső felhasználó közel sem ilyen érzékeny.

---

[16] PELTIER, Thomas. R: Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management, 2016

[17] Uo.

A biztonságérzet csökkenésével egyre több biztonsági és biometrikus rendszert vezetnek be a világon. A felhasználók általi elfogadottság szorosan együttjár azzal, hogy tudják-e használni a rendszert. Jelen cikkben két hipotézist teszteltünk:

H1: A fennakadás gyakorisága és a rendszer megítélt használhatósága között összefüggés van.
H2: Az emberek elfogadási küszöbe több nagyságrenddel magasabb, mint a gyártók által az eszközre megadott FRR – téves elutasítási értéke.

Mindkét hipotézist igazoltuk, és ezzel bizonyításra került, hogy a forgatókönyvi teszteknél mért valós FRR értékek ebben a tartományban értékelhetők. Habár a műszaki paramtérek fontosak a döntésben, ezekhez a legfontosabb mutatókat a cikkben össze is gyűjtöttük és megmutattuk, de nem mindig a műszaki adatok (paraméterek) a fontosak, ahogyan mutatja a kutatásunk is, az egyéni felhasználók kevésbé érzékenyek, mint a hitelesített FRR.

Az adott biztonsági körülmények között meg kell határozni, hogy a felhasználók milyen elfogadási értéke felel meg az üzleti döntéshozóknak és erre az értékre lenne szükséges a biometrikus beléptető rendszereket igazítani. Az is kiderült, hogy oktatással, az információk átadásával az elfogadottság szignifikánsan javítható. A szakirodalomban is legfontosabbnak egy ilyen rendszer bevezetése során a bevezetésnél megfelelő képzést és tréninget a későbbiekben pedig a körültekintő kontrollt látták[18].

A felhasználók elfogadása a technológiával kapcsolatosan egyértelműen tettenérhető egy ERP vagy HRIS rendszer bevezetése során is. Azzal, hogy számszerűsítettük, hogy az emberek mintegy 3-5%-os kényelmetlenséget még jellemzően elfogadnak, ez az érték várhatóan alkalmazható menedzsment rendszerek és szoftverek bevezetésénél és szervezetfejlesztési eseteknél is. Egyidejűleg az employee journey mapping elemzéseknél is alkalmazható az eredményünk. Ez azt jelenti, hogy tréning és az adott rendszerhez való elköteleződés javítása nélkül ilyen mértékű kényelmetlenséget még különösebb elégedettség csökkenés nélkül fogadnak a munkavállalók.

Felhasznált irodalom:

- CAVUSOGLU, Huseyin – CAVUSOGLU, Hasan – SON, Jai-Yeol – BENBASAT, Izak: Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. In: Information & Management, 2015, 52 évf. , pp. 385-400.
- DILLON, Andrew – MORRIS, Michael: User acceptance of new information technology: theories and models. In: Annual Review of Information Science and Technology, 1996. 31. évf. pp. 3-32.

[18] CAVUSOGLU, Huseyin– CAVUSOGLU, Hasan– SON, Jai-Yeol– BENBASAT, Izak: Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & Management, 2015, 52. évf., pp. 385-400.

- FAWCETT, Tom.: HP Laboratories Palo Alto. (2003, Január 7.). Retrieved április 1., 2018., from ROC Graphs: Notes and Practical Considerations for Data Mining Researchers: http://www.hpl.hp.com/techreports/2003/HPL-2003-4.pdf (Letöltés ideje: 2018. 03. 16)
- HANKA László: A Doddington-féle 30-as szabály, biometrikus rendszerek megbízhatóságának statisztikai elemzése. In: Tavaszi Biztonságtechnikai Szimpózium 2013, Budapest, Óbudai Egyetem, 2013
- HANKA László – WERNER Gábor: Using the Beta-Binomial Distribution for the Analysis of Biometric Identification, 2015, pp. 209-216.
- HORVÁTH Tamás – KOVÁCS Tibor: Kockázatértékelési módszerek, azok alkalmazási lehetőségei a fizikai védelem területén. In Tavaszi Biztonságtechnikai Szimpózium 2013, Budapest: Óbudai Egyetem, 2013
- (pp. 1-10.)
- ISO/IEC: ISO/IEC 19795-1 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. Svájc, (2006, április)
- ISO/IEC: ISO/IEC 19795-6:2012(E). Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation. Svájc, 2012
- JAIN, Anil. K. – FELLOW, Arindam Ghosh R. – PRABHAKAR, Salil: An Introduction to Biometric Recognition. In: EEE Transactions on Circuits and Systems for Video Technology, 2014, 14. évf. 1. sz., pp. 4-20.
- KOVÁCS Tibor – OTTI Csaba – MILÁK István: A biztonságtudomány biometriai aspektusai. In A biztonság rendészettudományi dimenziói: Változások és hatások, Pécs, Magyar Rendészettudományi Társaság, 2012, pp. 485-496.
- MICHELBERGER Pál–HORVÁTH, Zs: Security aspects of process resource planning. In: Polish Journal of Management Studie, 2017, pp. 142-153.
- NAZARETH, D. – CHOI, J.: A system dynamics model for information security management. In: Information & Management, 2015, pp. 123-134.
- OTTI, Csaba: Comparison of biometric identification methods. In: 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara, 2016
- OTTI, Csaba: Why does it fail to operate? In Thinking Together: The economy in practice, Budapest, Óbudai Egyetem, 2017, pp. 45-66.
- PELTIER, Thomas. R: Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press, 2016
- SAFA, Sohrabi. Nader – VON SOLMS, Roussouw: An information security knowledge sharing model in organizations. Computers in Human Behavior, 2016, pp. 442-451.
- SENNEWALD, Charles A. – BAILLIE, Curtis: Effective Security Management, Butterworth-Heinemann, Elsevier, 2015

- SHIMON, Modi K.: Biometrics in Identity Management: Concepts to Applications, , Norwood, Artech House, 2011
- SHPAK, Nestor – SATALKINA – Liliya – SROKA, Włodzimierz –HITTMAR, Stefan: The Social Direction of Enterprises's Innovation. In: Polish Journal of Management Studies, 2017, pp. 187–201.
- SOOMRO, Zahoor Ahmed – SHAH, Mahmood Hussain – AHMED, Javed: Information security management needs more holistic approach: A. In: International Journal of Information Management, 2016, pp. 215-225.
- SPRINGER: Security and Privacy in Biometrics. Springer, London Heidelberg New York Dordrecht, Springer, 2013.
- SROKA, W. – CYGLER, J. – GAJDZIK, B.: The Transfer of Knowledge in Intra-Organizational Networks: A Case Study Analysis. In: Organizacija, 2014, pp. 24-34.
- STAN Z. Li, A. K.: Encyclopedia of Biometrics - Second Edition. Springer, New York Heidelberg Dordrecht London, Springer, 2015

DR. TÚRI VIKTÓRIA

A TERRORISTÁK PSZICHOLÓGIAI ÉS BIOLÓGIAI JELLEGZETESSÉGEI ÉS KIVÁLASZTÁSI MÓDSZEREI[1]

Bevezetés

Az elmúlt években szinte nem telt el úgy hét, hogy ne hallottunk volna valamilyen terrorcselekményről, melyet a világ különböző pontjain hajtottak végre terroristák. Robbantás tömegrendezvényeken, lövöldözés szerkesztőségekben, tömegbe hajtás autóval stb. És ez csak néhány módszer a széles repertoárból. Mi motiválja ezeket az embereket arra, hogy egy terrorista szervezet tagjaivá váljanak és ártatlan embereket gyilkoljanak meg például egy karácsonyi rendezvényen? Elmebeteg-e a terrorista? Hogyan zajlik a toborzásuk és a kiképzésük? Írásomban ezekre a kérdésekre próbálok választ találni.

A terrorista lelke és motivációi

A terrorizmus elleni harc problémáival foglalkozó hazai és külföldi szakértők 1972-től számolnak a nemzetközi terrorizmussal. Az 1972. évi müncheni nyári olimpiai játékokon a „Fekete Szeptember" elnevezésű palesztin terrorszervezet egy akciócsoportja megtámadta az izraeli olimpiai csapat szállását, majd több sportolót túszul ejtve a fürstenfeld-brucki repülőtéren tűzharcba keveredett a bevetett német rendőrökkel és katonákkal, akik öt terroristát lelőttek, hármat pedig elfogtak. A túszul ejtett izraeliek közül kilencen haltak meg a terrorakció során. Ez a tragikus esemény hívta fel a világ közvéleményének és a kormányok többségének figyelmét a terrorizmus óriási veszélyére és nemzetközivé válására.[2]

Lényegében ez a helyzet jellemezte a nemzetközi terrorizmus elleni küzdelemre való felkészülést 2001. szeptember 11-ig, a New York-i és a washingtoni, hatalmas áldozatokat követelő al-Kaida terrortámadásig. A moszkvai színházban és a metróban, Csecsenföldön, Oszétiában, Beszlán városában, a madridi pályaudvaron, Londonban, Egyiptomban, Szaúd-Arábiában, a Fülöp-szigeteken, Afganisztánban, Törökországban, Izraelben, Indiában és Indonéziában, valamint Afrika és Latin-Amerika számos országában. A 2001. szeptember 11-e után elkövetett, egyre nagyobb számú és egyre több áldozatot követelő terrortámadások világossá tették a haladó emberiség előtt az új típusú terrorizmus fokozódó veszélyét és az ellene történő határozott fellépés fontosságát, szükségességét. A haladó világ

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Szélsőségek, vallási szélsőségek Ludovika Kutatócsoport keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

[2] RESPERGER István – TÚRI Viktória: A terrorizmus és az aszimmetrikus hadviselés pszichológiai aspektusai, In: http://www.repulestudomany.hu/kulonszamok/2010_cikkek/Resperger_I-Turi_V.pdf (Letöltés ideje: 2018. 04. 26.)

politikusai egyetértettek abban, hogy ennek a fellépésnek határozottnak, gyorsnak, összehangoltnak és eredményesnek kell lenni.[3]

A múltban alkalmazott erők, eszközök és eljárások nem tudták meggátolni a nemzetközi terrorizmus akcióit és az újabb akciók előkészítését. Tehát új, jobban felkészült erőkre, új és hatékonyabb eszközökre, új és sikeresebb harci eljárásokra van szükség a nemzetközi terrorizmus elleni küzdelemben.

Kezdünk tehát hozzászokni ahhoz, hogy a napi híradásokban egyre gyakrabban szerepel valamilyen terroresemény. A média sok információt eljuttat hozzánk, de európai szemmel még most sem vagyunk képesek megérteni az ilyen cselekmények mögött húzódó motivációkat. Miért lesz valaki öngyilkos ily módon? Miért robbantja fel magát, sőt, egyáltalán miért csatlakozik olyan szervezetekhez, ahol a foglyul ejtett embertársainkat élve égetik el? Ami nehezíti a terroristák és öngyilkos merénylők motivációinak és pszichéjének a vizsgálatát, az a tény, hogy nem tudjuk őket a napi rutinjuk során kikérdezni, a kutatók nem lehetnek részesei egy terrorista szervezet mindennapjainak, természetes közegében tehát nem vizsgálható a terrorista, az öngyilkos merénylők pedig meghalnak az akciók során, így őket sem tudjuk kikérdezni. Az ezzel kapcsolatos kutatások így arra alapoznak, hogy az öngyilkos merénylő családjával esetleg sikerül interjút készíteni (lásd Julia Juzik orosz újságíró, aki csecsen öngyilkos merénylők családtagjaival beszélgetett) vagy egy sikertelen merénylet után az elkövetőt elfogják és kikérdezik. Ez még így is kevés információ. Sokan azt gondolják, hogy a terroristák pszichopaták, szociopaták, elmebetegek, őrültek stb. Sajnos azonban ezek a következtetések, feltételezések nem állják meg a helyüket. A terroristák sokszor ugyanolyan emberek, ugyanolyan „normális" emberek, mint bárki más. Ennek ellenére számos vizsgálat próbálta feltárni, hogy milyen lehet ezeknek az embereknek a pszichéje, illetve mi motiválja őket cselekedeteik végrehajtásában?

Érdemes lehet első körben a magyarázatokat az egyik legősibb ösztönünkben keresni, ami nem más, mint az agresszió. Az elmúlt évszázadok során rengeteg olyan erőszakos és agresszív eseménnyel kellett szembenéznie az emberiségnek (I., II. világháború, terrorista merényletek, 2001. szeptember 11. stb.), melyre nem is gondoltunk volna. Az I. világháborúban közel 10 millió ember vesztette életét, és 20 millió ember sérült meg. A II. világháborúban egyes számítások szerint 40-50 millióan haltak meg, bár ezek az adatok nem teljesen pontosak. Emberek követtek el emberek ellen olyan brutális támadást, kínzást, éheztetést, melyben ennyien haltak meg. Ma már látjuk, hogy az emberi agresszió szinte nem ismer határokat. Szociálpszichológiai kísérletek azt is megmutatták, hogy pusztán laboratóriumi körülmények között is képesek vagyunk az embertársunknak halálos áramütést adni (Milgram-kísérlet) vagy egy börtönkörülményeket imitáló szituációban is képesek vagyunk bántani társainkat (Zimbardo börtönkísérlete), de erről a későbbiekben még lesz szó.

Érdekes és nem elhanyagolható tény az, hogy az állatvilágban nem találunk ilyen durva agresszióra példát. Éppen ezért az agresszióval foglalkozó kutatások már

[3] RESPERGER István - TÚRI Viktória: A terrorizmus és az aszimmetrikus hadviselés pszichológiai aspektusai, In: http://www.repulestudomany.hu/kulonszamok/2010_cikkek/Resperger_I-Turi_V.pdf (Letöltés ideje: 2018. 04. 26.)

régóta foglalkoztatják nemcsak a pszichológusok, hanem a biológusok, szociológusok és etológusok fantáziáját is. De mit értünk pontosan agresszió alatt? Agresszió alatt összefoglalóan olyan viselkedésformákat értünk, amelynek célja vagy eredménye a másiknak való kár vagy sérelem okozása. Etológiai értelemben az agresszió fogalmát a következőképpen értelmezhetnénk: az egy fajhoz tartozó egyedek az erőforrás birtoklásáért küzdeni kezdenek egymással.[4] A Bartha-féle Pszichológiai Értelmező Szótár szerint az agresszió fogalma a következőképpen határozható meg: *„Támadó, erőszakos fellépés más személlyel szemben. Az analitikus irányzatok értelmezésében „más ember feletti hatalomra törő akarat", illetve a halálösztön megnyilvánulásai."*[5]

Az agresszió irányával, típusaival, kialakulásának okaival kapcsolatos kutatások közül ki kell emelnünk az agresszió irányával foglalkozókat, mely szerint az agresszió iránya háromféle lehet: irányulhat tárgyakra, emberekre vagy önmagunkra. Az önmagunk ellen fordított agresszió és indulat, vagy más szóval az öndestrukció ezen formája a pszichológusokat leginkább foglalkoztató terület, melyet sokszor figyelmen kívül hagyunk, pedig a különböző pszichoterápiák kapcsán a szakember sokszor találkozik ezzel a jelenséggel. Felmerülhet a kérdés, hogy például egy vallási okokból elkövetett öngyilkossági kísérlet ugyanígy sorolható-e ebbe a kategóriába, hiszen egy öngyilkos merénylőt teljesen más motiváció mozgat, mint egy Európában élő, krízisben lévő és ezért meghalni akaró embert.

Érdekességként említeném meg, hogy bár az agresszió az állatvilágban is meglévő jelenség, általában a létfenntartáshoz kapcsolható, míg az emberi agresszióra ez csak ritkán jellemző. Az emberek esetében az agresszió már bonyolultabb fogalmat takar, hiszen, mint ahogyan azt már a fentiekben említettem, nem mindegy annak iránya, illetve szándékossága.

Felmerülhet egy fontos kérdés: ösztönszerű-e az agresszió?[6] Rousseau A társadalmi szerződésben leírt elmélete szerint az ember alapvetően kedves jámbor lény, de a társadalom által létrehozott és magalkotott korlátok között nehezen találja helyét.[7]

Freud szerint azonban az emberrel együtt születik meg az Eros, az életösztön, illetve a Thanatos, vagyis a halálösztön. Freud elképzelése és elmélete alapján az agresszív törekvések tehát léteznek, ezért valamilyen formában a felszínre kell, hogy törjenek. Az a forma, amelyben az agresszió utat tör magának, személyenként, személyiségenként eltérő. Van, aki sportban találja meg a feszültség levezetésének módját, van, aki a nevetésben, humorban. Freud elmélete szerint az agresszív törekvések háttérbe szorítása erőteljes érzelmi feszültséget generál az emberekben, tehát a feszültség levezetése egyfajta katartikus élménnyel is jár.[8]

---

4 CSÁNYI Vilmos: Agresszió az állatvilágban, Natura Kiadó, Budapest, 1986.
5 BARTHA Lajos: Pszichológiai értelmező szótár, Akadémia Kiadó, Budapest, 1981. p. 10.
6 ARONSON Elliot: A társas lény, Budapest, Akadémia Kiadó, 2008.
7 ROUSSEAU Jean-Jacques: Társadalmi szerződés, Phőnix-Oravetz Kiadás, Budapest, 1947.
8 FREUD:Sigmund A halálösztön és az életösztönök, Belső Egészség Kiadó, 2011.

Az aszimmetrikus hadviselés pszichológiai háttere azonban jóval bonyolultabb, hiszen nem csupán Erosról és Thanatoszról, vagy létfenntartásról szól, hanem bonyolult szocializációs, vallási alapú, meggyőződésből elkövetett agresszív cselekedetekről van szó. Olyan emberek és csoportok destruktív cselekvéseiről beszélünk, akik pusztán vallási, ideológiai meggyőződésből, a médiát nagyon ügyesen felhasználva és azzal pánikot keltve nemcsak fizikai értelemben okoznak halált, hanem a túlélőkben is mély traumát hagynak a különböző videofelvételeken és újságcikkeken keresztül.

A háborúk, melyek évszázadok óta színezik az emberi történelmet, mennyire tekinthetők agresszív cselekedetnek? Hiszen a harcoknak csak kis hányada robbant ki fajfenntartás vagy élelemszerzés céljából. Sokkal inkább a hatalomvágy és a terjeszkedés, területszerzés motiválta az uralkodókat, vagy valamilyen vallási elképzelés ösztökélte őket arra, hogy háborút indítsanak a másik fél ellen. Azok a személyek, akik a háborúkban harcolnak, vajon milyen motivációs bázissal rendelkeznek? Mi motiválja őket arra, hogy számukra ismeretlen embereket lemészároljanak? Itt merül fel a következő igen fontos kérdés: a neveltetés, a gyermekkori szocializáció, a vallás milyen szerepet töltenek be az agresszív viselkedésformák kialakulásánál?

Ha belegondolunk, az agresszió mindig jelen van az ember életében, már gyermekkorától fogva: a szocializáció folyamán a szülők számos akadályt és tiltást eszközölnek a gyermekükkel szemben, hogy a társadalmi elvárásoknak megfelelő felnőtt embert neveljenek belőle. Az agresszió tehát folyamatosan körülvesz bennünket, néha céltalanul lebeg mellettünk hétköznapjainkban.

A vallás és az ennek kapcsán kialakult életmódbeli és kulturális különbségek szintén évszázadok óta jelen vannak mindennapjainkban.

A vallásnak tehát ambivalens szerepe van a világ életében, hiszen próbálja oldani az előítéleteket és a vallási csoportok közti különbözőséget, mégis különböző csoportosulásokat teremt. Egyes elképzelések szerint, ha nem lennének a Földön különböző vallások, megszűnnének az előítéletek és a vallási okokból elkövetett mészárlások. A vallás nemcsak hit az azt gyakorló ember számára, hanem kultúrájuk alapját is képezi, meghatározva ezzel az életvitelt és a hétköznapokat.[9]

Csányi Vilmos[10] szerint az állatvilágban fellelhető agressziótípusok némi módosítással az emberre is igazak lehetnek, de a létfenntartásért folytatott emberi agresszió igen ritka. Csányi a következőképpen csoportosítja az emberi agressziót:

1. Területvédő agresszió: ez a fajta az agresszió a kutatások szerint már bölcsődében illetve az óvodában is megfigyelhető, körülbelül kétéves kortól létezik.

2. Tulajdon- és birtokbavételi agresszió: másfél éves kor körül jelenik meg először, ilyenkor az agresszió még nyílt, a gyermek nem leplezi érzéseit.

3. Kívülállókkal, behatolókkal szembeni agresszió: minden ember az élete folyamán tartozik bizonyos csoportokhoz. Az adott csoport elképzeléseivel, normáival, működésével azonosulunk, egyetértük, így azokat a személyeket, akik

[9] ALLPORT Gordon: Az előítélet, Gondolat Kiadó, Budapest, 1977.
[10] CSÁNYI i. m.

nem tartoznak a mi csoportunkhoz, kívülállónak ítéljük meg, és ha úgy érezzük, hogy veszélyeztetik a mi csoportunkat, agresszív érzéseket táplálunk irányukba.

4. Agresszió a csoportban, rangsorban való előrejutásért: bizonyos mértékben egészséges ambíciókat takar.

5. Frusztrációs agresszió: ha valamilyen cselekedetünkben frusztrálva vagyunk, a frusztrációt okozó akadály leküzdése agresszív színezettel rendelkezik.

6. Behatoló/határkitapogató agresszió: az adott helyzetbe, környezetbe újonnan érkező személy exploráló agressziója.

7. Autoagresszió: az agressziónk nemcsak tárgyak vagy személyek felé, tehát kifelé irányulhat, hanem befelé önmagunk ellen is. Ilyen például az, amikor a hatalom nélküli, cselekedeteiben akadályoztatva lévő személy tehetetlenségében önmagát kezdi emészteni.

8. Normatív, erkölcsi elvérvényesítő agresszió: minden közösség, csoport, társadalmi egység igyekszik a saját elképzeléseit és akaratát érvényesíteni.[11]

Más perspektívából nézve, az agresszióval kapcsolatos kutatásokat két nagy részre bonthatjuk: az egyik Freud elképzelése, melyben az agressziót drive-ként értelmezi, tehát belső hajtóerőből, késztetésből fakadó tényező. Az agresszió, mint a drive-elméletek egyik alapja, a frusztráció-agresszió hipotézis, melynek értelmében, ha valamilyen cselekedetünkben akadályoztatva vagyunk, keletkezik egy agresszív drive, mely arra késztet bennünket, hogy az akadályt okozó személyt vagy tárgyat megsemmisítsük. Vagyis az agresszió egyfajta energia, amely egészen addig megmarad, amíg ki nem elégítjük. Ebből táplálkozik egy másik elmélet is, mely szerint, ha az agresszió egyfajta energia, akkor annak kielégítése katarzist is okoz. Kérdéses az, hogy ebben az agresszió-katarzis teóriában az agresszor által elkövetett tett esetleges szörnyű következményei, a látvány, melyet az erőszakos, agresszív viselkedésével okozott, mennyire fogják vissza az átélt katarzist.

A másik kiemelkedő magyarázat az agresszív viselkedésre a szociális tanuláselmélet, mely Bandura nevéhez fűződik. E szerint az elmélet szerint az agresszív viselkedés nem más, mint egyszerű utánzás. A gyermek például látja szüleit, akik egyfolytában egymással vitatkoznak, majd az óvodában, iskolában ő is alkalmazza ezeket az otthon látott és tanult elemeket[12].

A szociális tanuláselméletre igen jó példa az az eset, amely pár évvel ezelőtt keringett az interneten. A videóban egy négyéves kislány anyukája robbanószerkezetet erősít magára, majd búcsút vesz kislányától. Az édesanya, Reem Saleh al-Riyashit (†22) négy másik embert rántott magával a halálba, amikor felrobbantotta magát. A kicsi lány pedig azt mondja a videóban, hogy ő is követni fogja édesanyja példáját, akire nagyon büszke.

Az emberi agresszió és erőszak tehát igen összetett mechanizmus, melyben szerepe lehet a tanulásnak is, a gyermekkori szocializációs folyamatnak, valamint ösztöneinknek egyaránt. A terrorista szervezetek filozófiájához pedig tökéletesen illeszkedik az agresszió okozta félelemkeltés, mely súlyos döbbenetet vált ki a

[11] CSÁNYI i. m.

[12] PATAKI Ferenc: Pedagógiai szociálpszichológia, Gondolat Kiadó, Budapest, 1976.

lakosságból. Ezt a döbbenet- és félelemkeltő stratégiát a „terror" szó kezdőbetűi is magunkba foglalják[13]:

• T, mint tervezz: hosszú és precíz időszak előzi meg általában a végrehajtott akciókat, melynek a személyek felkészítése is része, illetve az adott országokban az alvó cellák aktiválása. Az előkészületek akár hónapokig is eltarthatnak, majd a pontos cél esetén 1-2 hét alatt megszervezhető a támadás.

• E, mint elrettents: olyan célpontot kell választani, amely az ország szempontjából kiemelt fontosságú.

• R, mint robbants: hátizsákot, tűzveszélyes anyagokat, tömeget, járművet, bármit.

• R, mint rombolj: a rombolás lényege, hogy minél erőteljesebb pszichológiai hatást tudjanak elérni és az emberekbe beépítsék a félelmet.

• O, mint okozz pánikot: a pánik mindig jó terepet kínál arra, hogy a következő akcióról elvonja a figyelmet.

• R, mint reklámozz: a média kiemelten fontos a terrorszervezetek számára, de még nagyobb hírverést kap bármilyen akció, ha azt egy nő hajtotta végre.

A rengeteg agresszív és megdöbbentő rombolásokat látván, a kutatók a terroristák motivációinak és pszichéjének vizsgálatakor próbáltak felállítani egy úgynevezett terrorista személyiségprofilt. A gondolat onnan származott, hogy ha a terroristákat bűnözőknek tekintjük, akkor a bűnelkövetők személyiségprofilja alapján könnyebben rájuk lehet bukkanni, ezzel is csökkentve a betoborzás kockázatát és megelőzni az esetleges terrorcselekményt.[14] Az FBI elkészítette a tipikus sorozatgyilkos profilját, mely a következőket tartalmazza: a tipikus elkövető általában fiatal, 18 és 32 év közötti. Gyermekkorára jellemző volt a kései ágybavizelés, valamint az állatkínzás és gyújtogatás is megjelent náluk. Általában zaklatott családi háttérben nőttek fel, ezért a sorozatgyilkosok nagy része bizonyos fokú személyiségzavarral is küzd.[15] A kérdés pusztán annyi, hogy ez a profil alkalmazható-e terroristák esetében is? Míg a 80-as évek kutatásai azt boncolgatták és állították, hogy a terroristák elmebetegek, addig mára már tudjuk, hogy ez egyáltalán nem így van, hiszen a terroristák képesek hosszú éveken át rejtőzködni és teljesen más életet élni egészen addig, ameddig nem aktiválják őket.[16]

A kriminológiai kutatások egyik legizgalmasabb része a biológiai, neurológiai, élettani és anatómiai vizsgálatok, melyek azt próbálták feltérképezni, hogy a terroristáknál fellelhető-e az átlagtól eltérő agyi aktivitás, agyterületi dominancia stb. A vizsgálatok az agresszióra való hajlamból indultak ki: a különböző hormonok és neurotranszmitterek arányait próbálták vizsgálni. Egyes vizsgálatok megállapították azt, hogy a bűnelkövetőknél kétszer-háromszor gyakrabban fordul elő az endokrin mirigyek megbetegedése: például a mellékvesekéreg túlműködése miatt kialakult Chusing-szindróma és a pajzsmirigyhez köthető hipertireózis vagy

---

[13] KŐSZEGVÁRI Tibor- RESPERGER István: A nemzetközi terrorizmus elleni küzdelem katonai tapasztalatai, ZMNE, egyetemi jegyzet, Budapest, 2006. p. 9.

[14] ZSIFKÓ Mariann: A terrorista profilja, In: http://old.biztonsagpolitika.hu/userfiles/file/PDF/zsifko_a_terrorista_profilja.pdf (Letöltés ideje: 2018. 04. 26.)

[15] U. o.

[16] Sz.n. :Kiból lesz terrorista? In http://7koznapi.blog.hu/2017/03/18/kibol_lesz_terrorista (Letöltés ideje: 2018. 04. 26.)

más néven golyva gyakran jár együtt például obszesszív-kompulzív magatartással.[17] A hormonok közül a tesztoszteron és az androgén hormonok felelnek az agresszívabb viselkedés kialakulásáért: a tartósan magas tesztoszteronszint csökkenti a szociális integrációra és kooperációra való hajlamot.[18]

A neurotranszmittereket érintő kutatások a szerotoninra, a dopaminra és a norepinephrinekre terjedtek ki. A szerotonin köztudottan felel a boldogságunkért, a jó kedvért, azért hogy szorongásmentesebben éljük a hétköznapjainkat. Az alacsony szerotonin szint fokozza a negatív gondolatokat és azok eluralkodását a személyen. Megállapították azt is, hogy a magas dopamin szinttel rendelkező egyének sokkal inkább keresik a szenzoros ingereket, veszélyes helyzeteket, mint társaik. Az alacsony szerotonin szint, a magas dopamin szint, valamint a norepinephrinek kiegyensúlyozatlansága antiszociális viselkedéshez vezethet.[19]

A terroristák személyiségének vizsgálatakor is több irányzat keletkezett. A pszichoanalitikus kutatások egyik irányvonala a nárcizmust állítja a középpontba. A nárcisztikus személyiség első látásra grandiózus és elsöprő, az ilyen személyek gyakran bejáratosak jó társaságokba és gyakran állnak a figyelem középpontjában. Az ilyen emberek túlzott jelentőséget tulajdonítanak saját énjüknek, eltúlozzák saját képességeiket és tehetségüket. Jó megjelenésűek és elsőre elbűvölő személyiségnek tűnnek. Nekik még a problémáik is speciálisak, és ezeket csak különleges emberekkel tudják megosztani és megbeszélni. Sokszor tűnnek beképzeltnek és arrogánsnak. Karizmatikus személyiségük kiváló lehet toborzásra. De mi húzódik valójában az ilyen személyiség hátterében?

A nárcisztikus embereket általában kora gyermekkorukban éri sérülés, mely az egészséges énkép kialakulását gátolja. A szülők általában rideg és elutasító légkörben nevelték gyermeküket, akikkel azt éreztették, hogy semmire sem jók, bármit is tesznek, mindenre alkalmatlanok. Bárminemű kritikára, tiszteletlenségre túlérzékenyen, időnként dühkitöréssel reagálnak.[20] Az empátia minden csírája hiányzik belőlük, így valóban magyarázat lehet a terrorista személyiségre, hiszen aki képes egy embert fejbe lőni vagy élve elégetni, abban nem sok empátia lehet. Az őt ért igazságtalanságokat agresszív cselekedetekkel próbálja levezetni és kompenzálni. Az instabil énkép pedig azzal győzködi, sőt gyógyítja önmagát, hogy az áldozat szerepéből (akit gyermekkorában megaláztak és meggyötörtek) átvált a morális elvek mentén cselekvő agresszor szerepébe.[21] Az elmélet tehát inkább gyermekkori traumákra épít, de bizonyos kutatások a felnőttkori traumákat is hangsúlyozzák, mint például a börtönben eltöltött évek, melyek hozzájárulhatnak a szélsőséges magatartásformák felvételéhez. Az 1980-as években keletkezett egy kutatás, melynek eredményeként a CIA egyik elemzője arra a következtetésre jutott, hogy a terroristák mindenféleképpen patológiás személyiségek és két típusuk létezik:[22] 1)

---

[17] PÓCZIK Szilveszter A terrorizmus biológiai és pszichológiai elméletei In http://www.vilagossag.hu/pdf/20070815112115.pdf (Letöltés ideje: 2018. 04. 26.)

[18] U.o.

[19] U. o.

[20] COMER Ronald J. A lélek betegségei – Pszichopatológia, Osiris Kiadó, Budapest, 2005. ISBN: 963-389-448-4

[21] PÓCZIK Szilveszter A terrorizmus biológiai és pszichológiai elméletei In http://www.vilagossag.hu/pdf/20070815112115.pdf (Letöltés ideje: 2018. 04. 26.)

[22] U. o.

Anarchista típus: gyakran szenvedett el bántalmazást a szülei részéről, ezért gyűlöletet érez szülei iránt. 2) Nacionalista típus: a szüleit, családját ért igazságtalanságokat próbálja megtorolni a külső, családon kívüli világban.

Más kutatás is azt hangsúlyozza, hogy a gyermekkorban elszenvedett traumák, illetve a serdülőkori, érzelmileg alapvetően is kiegyensúlyozatlan időszakban lévő fiatalok jobban bevonhatók egy terrorista szervezet életébe. Meghatározó lehet tehát:

- „A személyiségfejlődés további irányát meghatározó súlyos pszichés behatás gyermekkorban, ami a normális érzelmi fejlődést megakadályozza (sok terroristánál ez a szülők erőszakos halála, amit súlyosbít az, ha a gyermek személyesen éli meg szerettei elvesztését);
- serdülőkorban (a 10 és 14 éves kor közötti időszakban) az érzelmileg könnyen befolyásolható és tartást, elismerést kereső egyén — aki gyermekkora traumatikus élménye miatt úgynevezett „személyiségdeficitben" szenved — külső hatásra egy számára katartikus megvilágosodást jelentő, valamint életének értelmet adó eszméhez csatlakozik;
- az így fejlődő személyiség súlyos konfliktusokkal terhelt társadalomban nő fel, ahol a közösség érdekeinek érvényesítésére alkalmazott eszközök rendszerében az erőszak jelen van."[23]

A terrorista szervezetbe jelentkezőknél azonban nemcsak a személyiséget érdemes vizsgálni, hanem a motivációkat is:

1. fontos az aktív cselekvés lehetősége,
2. a valahová tartozás igénye,
3. egyfajta társadalmi státusz elérése,
4. anyagi jutalom,
5. a feltételezett igazságtalanság elleni küzdelem és az erkölcsi rend helyreállítása,
6. identitáskeresés, melyhez egy erős csoport és egy karizmatikus vezető hozzájárulhat,
7. bosszú, szégyen, az elvesztett saját, vagy a család becsületének visszaszerzése.[24]

Ha az eddig leírtakat vesszük figyelembe, igazából csak találgatunk, hogy van-e pszichopatológiai háttere a terrorizmusra való hajlamnak, de egyelőre azt látjuk, hogy klinikai értelemben a terroristák nem elmebetegek. Sőt, ezek a szervezetek inkább el is kerülik a mentálisan beteg személyeket, mert alkalmazásuk és bevetésük igen kockázatos. Az előre megtervezett terrorakciók végrehajtásához szükséges egyfajta pszichés stabilitás, kitartás és szakmai rátermettség is. Kifejezetten olyan embereket keresnek, akik jártasak az internet világában és jól tudják használni a

[23] TÜTTŐ Szabolcs: Az öngyilkos terrorizmus stratégiai jelentősége, személyiség-lélektani háttere és szociológiai vonatkozásai, In: http://epa.oszk.hu/02400/02463/00003/pdf/EPA02463_hadtudomanyi_szemle_2008_3_072-086.pdf, p. 77. (Letöltés ideje: 2018. 04. 04.)

[24] PÓCZIK Szilveszter A terrorizmus biológiai és pszichológiai elméletei In http://www.vilagossag.hu/pdf/20070815112115.pdf (Letöltés ideje: 2018. 04. 26.)

különböző közösségi oldalakat is[25]. Alapvetően nem tudunk felállítani tipikus terrorista profilt, de ami elmondható, hogy fiatal, 18-25 éves, általában nőtlen, nagyvárosi, felső- vagy középosztálybeli, felsőoktatásban tanult vagy tanuló férfiak lesznek a terrorista csoportok tagjai. Nyilván az alacsonyabb pszichikai fejlettségi szinttel rendelkezőknek biztonságot adhat egy ilyen szervezethez való csatlakozás, de azok is könnyebben bevonhatók, akik zárt, szigorú normák között nevelkedtek, ahol a szülők a nevelés eszközeként főként a büntetést alkalmazták.[26]

Továbbra is nyitva marad azonban két kérdés: mi motiválja akkor ezeket a fiatalokat, hogy csatlakozzanak egy ilyen szervezethez, és hogy az öngyilkos merénylők motivációi miben gyökereznek?

Fontos kérdés az, hogy hogyan történik a terroristák és az öngyilkos merénylők toborzása és kiképzése. A kutatások szerint a terrorista szervezetekhez való csatlakozás motivációi igen széles spektrumon mozognak: szégyen, szerelem, meggyőződés, vallási fanatizmus, megalázottság, a becsület visszaszerzése, vagy egyszerűen nincs más választás, például a női terroristák esetén.

Dounia Bouzar és Carol Rollie Flynn cikkükben részletesen beszámolnak azokról a toborzási stratégiákról, melyeket a terrorszervezetek alkalmaznak beszervezésre. Hét fő indokot, beszervezési módot, narratívát különítettek el írásukban egy Franciaországban végzett kutatás alapján.[27]

1. A „jobb világ” narratíva: e szerint az alternatíva szerint azzal az érvvel próbálnak embereket toborozni a szervezetbe, hogy egy új társadalmat tudnak felépíteni, melyben az egyenlőség, testvériség és szolidaritás uralkodik majd.

2. A „Teréz anya” narratíva: a toborzók ebben az esetben olyan fiatalokat vesznek célkeresztbe, akik olyan területeken képzelik el magukat vagy olyan területeken dolgoznak, ahol embereken tudnak segíteni: pl. nővérek, ápolók, szociális területen dolgozók stb. A toborzás során olyan szörnyűséges tartalommal ellátott videókat mutatnak nekik, amelyben például az Asszad csecsemőket gázosít el. Ez olyan mértékű morális sokkot okoz, hogy meggyőzhetővé válhatnak az emberek arra, hogy ezen csak a dzsihádizmus segíthet.

3. A „Megmentő/Megváltó” narratíva: amikor a toborzó olyan személlyel találkozik, aki nemrég elveszített egy számára kedves személyt, akit nagyon szeretett, és kihasználja az embernek azt a vágyát, hogy újra találkozhasson vele. A toborzók különböző videókat mutatnak ilyenkor is a jelölteknek, amely videók tartalma ebben az esetben az újraegyesülésre fókuszál, mely egy kis nyugalmat ad a veszteséget átélt fiatal háborgó lelkében, ezzel is enyhítve bánatát. A Paradicsomban pedig minden másként lesz, együtt lehetnek a családjukkal, az elveszített szeretett személlyel egy varázslatos helyen újra.

---

[25] ZSIFKÓ Mariann: A terrorista profilja, In: http://old.biztonsagpolitika.hu/userfiles/file/PDF/zsifko_a_terrorista_profilja.pdf (Letöltés ideje: 2018. 04. 26.)

[26] BOLGÁR Judit - SZTERNÁK György: A terrorizmus társadalmi és személyiség lélektani háttere, In: http://docplayer.hu/23966122-A-terrorizmus-tarsadalmi-es-szemelyiseg-lelektani-hattere.html (Letöltés ideje: 2018. 04. 23.)

[27] BOUZAR, Dounia – FLYNN Carol Rollie: ISIS Recruiting: It’s Not (Just) Ideological, In: https://www.fpri.org/article/2017/09/isis-recruiting-not-just-ideological/ (Letöltés ideje: 2018. 04. 06.)

4. A „Házasság narratíva”: ezzel a módszerrel az olyan fizikailag és pszichológiailag is gyenge nőket próbálják toborozni, akik átestek már valamilyen szexuális bántalmazáson vagy fizikai erőszaknak voltak kitéve. A toborzók azt hirdetik, hogy „találd meg azt a férjet, aki soha nem hagy majd el téged”.

5. A „Lancelot narratíva”: ennek a módszernek a céljpontjai főként azok a férfiak, akik hisznek a hősökben, a hősies viselkedésben és a történelmi karakterekben. Bátorító videókat mutatnak nekik hős harcosok történeteiről, melyekhez domináns és motiváló, erőteljes zenei hátteret tesznek.

6. A „Zeusz narratíva”: ez a toborzási módszer a mindenhatóság érzésére épít és főként azokat a fiatalokat használja fel, akik életüket kockázatokkal tarkítva élik: kábítószerek, védekezés nélküli szex, túl gyors vezetés stb. Úgy viselkednek, mintha mindenhatók lennének – próbálgatják és feszítik a határaikat. Nem vetik alá magukat Isten akaratának, de az Isten nevében tesznek dolgokat.

7. Az „Erőd narratíva”: a toborzók célpontjai ebben az esetben azok a kamasz vagy fiatal felnőttek, akiket rögeszmés szexuális vágyak hajtanak, ezért félnek attól, hogy ez kiderül, és a társadalom kirekeszti őket. Ezek a férfiak lehetnek hetero- vagy homoszexuálisok, de egyes esetekben pedofilok is. Az „Erőd”, mint elnevezés arra utal, hogy ha a fiatalok belépnek a szervezetbe, ott megtalálhatják önmaguk egy jobb változatát, amely megvédi őket attól, hogy szexuális rögeszméiket kövessék.[28]

A fentiekből nagyon jól kirajzolódik az, hogy a különböző terrorszervezetek toborzói profi szinten űzik a beszervezést. A toborzók célcsoportja korosztályok szerint könnyen beazonosítható, általában a húsz év körüli fiatalok a legfogékonyabbak. Gyakori még az árva gyerekek beszervezése például Palesztinában, míg Csecsenföldön a kislányokat már igen fiatalon eladják, választásuk tehát nincs, vagy egyéb erőszakos eszközökkel veszik rá őket a csatlakozásra. A stratégia folyamatosan igazodik a kor elvárásaihoz és szokásaihoz, mivel az emberek ebben az életkorban rendszerint egy eszmét keresnek, egy csoportot, amelyhez tartoznak. Ebben az időszakban a kamaszok érzelmileg nagyon befolyásolhatók. Érdemes kicsit közelebbről megvizsgálnunk, hogy mi történik pontosan egy kamasz lelkében ilyenkor, mert ezzel érthetővé válik fogékonyságuk a különböző szervezetek irányába. A hormonrendszer működésének beindulása élettanilag is okoz nehéz időszakokat a pubertás életében. Olyan kérdésekre keresik a választ, hogy mi lenne, ha ezt vagy kipróbálnám, megcsinálnám, megvalósítanám stb. Kíváncsiak arra, hogy bizonyos problémákat képesek lennének-e megoldani. Kritikai képességük ebben az időszakban virágzik, mely rengeteg konfliktus forrása lehet. Ugyanakkor a szülői háttértámogatásra szükségük van. Ha ez hiányzik vagy nem tökéletes, jól jöhet egy csoportosulás, egy szervezet, ami segít nekik ebben.

2014-ben Franciaországban készült egy elemzés arról, hogy egyes emberek miért csatlakoznának radikális csoportokhoz. Négy területet emeltek ki a kutatást követően, amelyre az elemzés során derült fény:

1. Az üzenet testre szabása: A toborzók egyre kifinomultabbá váltak és válnak, már olyan profi technikákat használnak, mint a hivatásos hírszerzők. A toborzók egyszercsak új barátként jelentkeznek az interneten, beszélgetéseket kezdeményeznek a jelöltekkel azzal a céllal, hogy értékeljék a beszervezés lehetőségeit és megbízható kapcsolatot építsenek ki velük. Ha ez megtörtént, a

[28] BOUZAR – FLYNN i.m.

fentiekben már említett hét narratíva/toborzó történet közül kiválasztják a személy számára legmegfelelőbbet. Mindegyik narratíva azonban színezett érzelmekkel, megtalálható benne az ideális csoporthoz való tartozás élményének fontossága.

2. Virtuális és valós kapcsolatok: A XXI. században a virtuális világnak köszönhető kapcsolatok virágzása egyre dominánsabb. Ugyanakkor e közösségi oldalakon való kapcsolatok felvételét sok esetben megelőzheti valódi személyes találkozás is.

3. Az újoncok kora, neme és társadalmi osztályai: A vizsgált mintában minden társadalmi-gazdasági osztály képviseltette magát. A jelöltek sokszor származtak nyomornegyedekből, de voltak és vannak középosztálybeli családokból és a gazdagabb környezetből érkezők is.

4. Vallási meggyőződései: A vizsgált mintában a jelentkezők 44 százaléka ateista, 30 százalékuk keresztény, 24 százalékuk muszlim és 2 százalékuk zsidó volt.

Fontos megemlítenünk, hogy a terrorszervezetekben már viszonylag régóta alkalmaznak női terroristákat is, akik a leírások szerint sokszor jóval kegyetlenebbek és indulatosabbak férfi társaiknál. Általában az öngyilkos merénylők, és ezen belül is a nők bevetése az ilyen jellegű műveletekben több szempontból is „logikus”:

1. az öngyilkos merénylők alkalmazása olcsó,
2. a kiképzésükre szánt idő rövid;
3. az öngyilkos merénylők egyszerű műveleteket hajtanak végre,
4. rendkívül nagy pusztítást okoznak,
5. nagyon komoly médiafigyelmet kap, főleg akkor, ha nő volt az elkövető. A különböző terrorista szervezetek pedig nagyon szeretik az effajta hírverést hiszen addig is róluk beszél az egész világ,
6. ha a merénylet sikeres volt, tehát nem gondolta meg magát a merénylő, akkor nincs lehetőség a kihallgatására (Sokszor éppen emiatt távirányítással is fel lehet robbantani ezeket a bombákat.),
7. az a pszichológiai sokk, amit egy női öngyilkos merénylő okoz, sokkal markánsabb és hosszabb távon hat,
8. a nők könnyebben félre tudják vezetni a biztonságra törekvő szakembereket: bő ruha, kismama álca stb,
9. a nőkkel szembeni sztereotípiák is helyzeti előnyt jelentenek: a nők gyengék és védtelenek,
10. a női elkövetők növelik a férfijelentkezők számát a szervezetbe, ösztönzően hat rájuk.

Az eddig leírtakból jól körvonalazódik az, hogy a terrorista szervezetek mentálisan egészséges embereket keresnek és ehhez igazították rendkívüli toborzó technikáikat. De mi történik a betoborzott emberekkel, hogyan formálják a kiválasztott, leendő, potenciális terroristákat? Noam Chomsky részletesen ír arról, hogy hogyan lehet embereket általánosságban manipulálni, melyből néhány pontot érdemes lehet ebben a kontextusban is megemlíteni. Ebben fontos szerepe van például egy karizmatikus vezetőnek, akit szinte gondolkodás nélkül követnek hívei. Ez a karizmatikus vagy politikai vezető megmentői szerepben is tetszeleg, aki egy szebb jövőt tud hozni vezetésével a világra. Ebből következik a másik nagyon fontos tény: el kell hitetni az emberekkel, hogy minden, ami jelenleg van, az rossz. Ha az

aktuális generációnak nem is lesz jobb, de jobb lesz majd a gyermekeiknek. Mindehhez az szükséges, hogy az embereket elszigetelten, az érzelmeikre hatva „neveljék" a csatlakozás után. A terrorista szervezetek bizonyos esetekben ezt erősítik különböző drogokkal és testi bántalmazásokkal is. Kiemelt fontosságú még a nyájszellem erősítése is: az egyénben fel kell ébreszteni a szégyen- és tehetetlenség-érzetet, és alternatívaként tudatosítani kell az igazodási, csatlakozási kényszert. Az egyéniségeket nélkülöző nyájat mindig könnyebb irányítani, ellenőrizni és befolyásolni.[29]

A nyájszellem és a konformitás vizsgálata már a múlt század közepén felkeltette a szociálpszichológusok érdeklődését, hiszen a II. világháború okozta mészárlást és az azt övező döbbenetet magyarázni kellett valamivel. Három ismert vizsgálat is említésre méltó lehet, mely segíthet jobban megérteni a terroristák kiképzését és személyiségük formálását. Az első ilyen kísérlet Solomon Asch nevéhez fűződő, úgynevezett „vonalas kísérlet". 1955-ben végezte vizsgálatát, melyben egy vonalat mutatott kísérleti alanyainak, akiknek az volt a feladata, hogy hasonlítsák össze a vonal hosszát három másik vonallal. A kísérletben természetesen voltak beavatott résztvevők is, akiknek a kísérleti személy előtt szándékosan rossz vonalat kellett kiválasztaniuk, mellyel nem egyenlő hosszúságú az eredeti, referencia vonal. A nem beavatott résztvevőnek tehát döntenie kellett: a csoportra hallgat vagy a józan eszére. Az eredmény meglepő volt: a kísérletben résztvevők egyharmada engedett a csoportnyomásnak. Asch sokféle módon próbálta a kísérletet megismételni, például változtatta a beavatott csoport létszámát hol nagyobbra, hol kisebbre. Az eredmények azonban nem változtak. Asch az eredmények alapján több csoportra bontotta a kísérleti alanyokat, de a lényege talán az, hogy társas lények vagyunk, szükségünk van a pozitív visszajelzésre és elismerésre, ezért engedünk a csoport nyomásának.[30]

A másik vizsgálat a világszerte elhíresült áramütéses vizsgálat, mely Stanley Milgram nevéhez fűződik. Az eredeti vizsgálatot 1961-ben végezte el az amerikai Yale Egyetem kutatója, három hónappal azután, hogy az egyik leghírhedtebb náci háborús bűnös, Adolf Eichmann pere lezajlott[31]. A második világháborút követő perek során gyakran hangzott el az a mondat, hogy „én csak parancsot teljesítettem". Ez indította el annak az igényét, hogy pszichológusok megvizsgálják, az emberek mennyire képesek behódolni a hatalomnak, a tekintélynek. A hatalomnak való engedelmesség tényleg képes-e az emberből szörnyet kreálni?

Ennek kiderítésére önkénteseket toborzott, akiknek a kísérlet vezetője azt az utasítást adta, hogy „tanárokként" rossz válasz esetén egyre erősödő áramütésekkel büntessenek egy elzárt szobában lévő személyt, akit hallanak ugyan, de látni nem látnak. A szenvedő alany természetesen nem kapott ténylegesen áramütést, neki csak el kellett játszania a fájdalmat. A kísérleti alanyok azonban ezt nem tudták, ők abban a hiszemben nyomták meg az áramütést adó gombot, hogy azzal tényleg ártanak a másik szobában ülőnek. A kísérleti személyek előtt egy olyan készülék volt, amely

---

[29] CHOMSKY, Noam: Titkok, hazugságok, demokrácia. David Barsamian interjúkötete Független Média Kiadó, 2005. p. 76. ISBN 9789638675309, Lásd még: Hatalom és terror. Előadások és interjúk 9/11 után Független Média Kiadó, 2005.

[30] ARONSON Elliot: A társas lény, Budapest, Akadémia Kiadó, 2008.

[31] http://www.origo.hu/tudomany/20170316-lengyelorszagban-is-elvegeztek-a-milgram-kiserletet.html (Letöltés ideje: 2018. 04. 11.)

különböző erősségű áramütést adott a beépített személyeknek. A kísérleti alanyok tudták, hogy az adott gomb megnyomásával milyen sérüléseket és mekkora fájdalmat okozhatnak a másik személynek. azt is tudták, hogy hány volt jelent halálos áramütést. Az eredmények borzasztóan elkeserítő képet adtak az emberi természetről: a kísérletben részt vevő 40 személy 65 százaléka vakon követte a kísérletvezető parancsát, és elment egészen a 450 voltos áramütés adásáig. Az sem zökkentette ki őket feladatukból, hogy közben a színész folyamatosan jajveszékelt és az életéért könyörgött. A kísérlet az egész világon óriási felháborodást váltott ki, éppen ezért sokan megismételték. Sajnos ugyanarra az eredményre jutottak.[32]

Végül még egy említésre méltó kísérlet: Zimbardo börtönkísérlete, melyből filmet is készítettek. Fiatal egyetemistákat toboroztak egy olyan kísérletbe, ahol a személyek egy része két hétig börtönőr lett volna, másik része pedig két hétig fogvatartott. A kutatást az Amerikai Egyesült Államok Haditengerészete rendelte meg és finanszírozta. Magyarázatot kerestek arra, hogy a haditengerészet és a tengerészgyalogság börtöneiben miért van annyi összetűzés az őrök és a fogvatartottak között. Zimbardo és csapata azt az elméletüket próbálták kísérleti úton bizonyítani, miszerint mind a börtönőrök, mind a foglyok meghatározott viselkedésformákat vesznek fel, amelyek az adott körülmények között a szituáció romlásához vezetnek.

A résztvevőket alaposan megszűrték: újsághirdetésen keresztül lehetett jelentkezni, majd vizsgálatok sora következett. Zimbardoék a tesztek alapján a legstabilabb, pszichésen és testileg is legegészségesebb embereket választották ki. A kísérletet azonban le kellett fújni, mert a börtönőrt játszó kiválasztott emberek olyan erőteljesen bántalmazták társaikat, hogy sokan közülük a kísérlet után terápiára jártak.[33]

Ha kísérleti közegben ennyire brutálissá válik az ember, mit várhatunk tényleges, éles, valós szituációban? Az emberek egyharmada miért nem merte felvállalni a véleményét a vonalas kísérletben? Az emberek 65 százaléka miért ölte meg áramütéssel embertársát? A börtönőr szerepet játszók miért bántalmazták társaikat? Ahogy azt már Hobbes óta tudjuk: „homo homini lupus” vagyis ember embernek farkasa.

Összefoglalás

A terroristákról tehát továbbra sem mondhatjuk el, hogy elmebetegek lennének, hiszen a hosszú évekig tartó bujkálás, az szakmai-műszaki ismeretek, alvó cellaként a közösségbe való beilleszkedés és a türelem képessége arra, hogy aktiválják őket, egy pszichésen instabil embernek nem feltétlenül sikerülne, hiszen betegségével csak felhívná magára a figyelmet. Nagy problémát jelent, hogy a terrorista csoportok toborzó stratégiái egyre tökéletesebbek lesznek és a közösségi médiát is felhasználva egyre precízebben találják meg a bevonható emberek körét. Természetesen egyes vizsgálatok beszámolnak arról is, hogy nem mindenki marad a terrorista csoport tagja, akadnak elhagyók is, akik rájönnek arra, hogy nem azt

[32] U. o. (Letöltés ideje: 2018. 04. 11.)
[33] ARONSON, Elliot: A társas lény, Akadémia Kiadó Zrt., Budapest, 2008.

kapják, amit ígértek nekik. De ez a ritkább. A XXI. század legnagyobb kihívásai között ezért továbbra is ott szerepel a terrorizmus felszámolása és megelőzése.

Felhasznált irodalom:

- ALLPORT, Gordon: Az előítélet, Gondolat Kiadó, Budapest, 1977.
- ARONSON, Elliot: A társas lény, Akadémia Kiadó Zrt., Budapest, 2008.
- BARTHA Lajos: Pszichológiai értelmező szótár, Akadémia Kiadó, Budapest, 1981.
- BOLGÁR Judit – SZTERNÁK György: a terrorizmus társadalmi és személyiség lélektani háttere In: http://docplayer.hu/23966122-A-terrorizmus-tarsadalmi-es-szemelyiseg-lelektani-hattere.html (Letöltés ideje: 2018. 04. 23.)
- BOUZAR, Dounia – FLYNN Carol Rollie: ISIS Recruiting: It's Not (Just) Ideological In: https://www.fpri.org/article/2017/09/isis-recruiting-not-just-ideological/ (Letöltés ideje: 2018. 04. 06.)
- COMER Ronald J.: A lélek betegségei, Osiris Kiadó, Budapest, 2005. ISBN 963-389-448-4
- CHOMSKY, Noam: Titkok, hazugságok, demokrácia. David Barsamian interjúkötete Független Média Kiadó, 2005. ISBN 9789638675309
- CHOMSKY, Noam: Hatalom és terror. Előadások és interjúk 9/11 után Független Média Kiadó, 2005.
- CLAUSEWITZ, Carl von: A háborúról I. kötet. p. 37.
- CSÁNYI V.: Agresszió az állatvilágban, Natura Kiadó, Budapest, 1986.
- ELLIOT, M.: Lessons from the Rubble In: Time September 1, 2003. p.22.
- FREUD Sigmund: A halálösztön és az életösztönök, Belső Egészség Kiadó, 2011. ISBN 9786155144042
- KŐSZEGVÁRI – RESPERGER: A terrorizmus elleni küzdelem katonai tapasztalatai Budapest, 2006. p. 50. ZMNE Egyetemi jegyzet
- PATAKI Ferenc: Pedagógiai szociálpszichológia, Gondolat Kiadó, Budapest, 1976.
- PÓCZIK Szilveszter: A terrorizmus biológiai és pszichológiai elméletei, In http://www.vilagossag.hu/pdf/20070815112115.pdf (Letöltés ideje: 2018. 04. 26.)
- RESPERGER István – TÚRI Viktória: A terrorizmus és az aszimmetrikus hadviselés pszichológiai aspektusai, In:http://www.repulestudomany.hu/kulonszamok/2010_cikkek/Resperger_I-Turi_V.pdf (Letöltés ideje: 2018. 04. 26.)
- ROUSSEAU Jean-Jacques: Társadalmi szerződés, Phőnix-Oravetz Kiadás, Budapest, 1947.

- Sz.n.: Kiből lesz terrorista? In http://7koznapi.blog.hu/2017/03/18/kibol_lesz_terrorista (Letöltés ideje: 2018. 04. 26.)
- TÜTTŐ Szabolcs: Az öngyilkos terrorizmus stratégiai jelentősége, személyiség-lélektani háttere és szociológiai vonatkozásai, In:http://epa.oszk.hu/02400/02463/00003/pdf/EPA02463_hadtudomanyi_szemle_2008_3_072-086.pdf p. 77. (Letöltés ideje: 2018. 04. 04.)
- ZSIFKÓ, Mariann: A terrorista profilja, In: http://old.biztonsagpolitika.hu/userfiles/file/PDF/zsifko_a_terrorista_profilja.pdf, (Letöltés ideje: 2018. 04. 26.)
- http://www.origo.hu/tudomany/20170316-lengyelorszagban-is-elvegeztek-a-milgram-kiserletet.html (Letöltés ideje: 2018. 04. 26.)

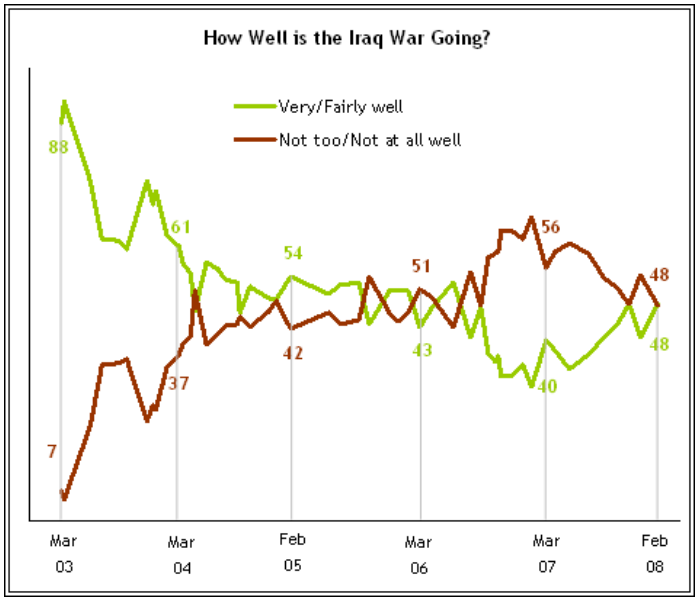
CSEHI GÁBOR

ASZIMMETRIKUS KONFLIKTUSOK ÉS AZ EGÉSZSÉGBIZTONSÁG

Megítélésem szerint, ha meg akarunk nyerni egy aszimmetrikus konfliktust - sok egyéb mellett – magas fokon szükséges biztosítanunk az egészségügyet, az egészségbiztonságot is.

Ez az igény független attól, hogy az aszimmetrikus konfliktust[1] hol kell megvívnunk: a hátországban vagy ellenséges területen. A háborús viszonyok között a katonai egészségügy a mérvadó. Ugyanakkor egy, a saját hátországunkban zajló konfliktus, egy ott elkövetett/elszenvedett terrortámadás esetén a civil egészségügynek kell a válaszintézkedéseket megtennie, a sérülteket ellátnia, a konfliktus ezen szintjét megnyernie.

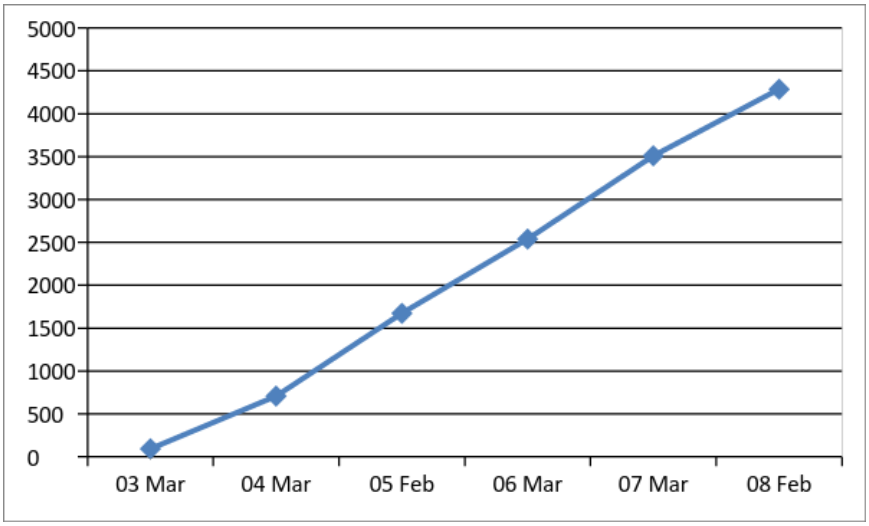
Véleményem szerint a nyugati társadalmak érzékenyek a (humán) veszteségre. A társadalom és ebből kifolyólag a politikai vezetés érzékenyen reagál minden egyes elhunytra. Ha megvizsgáljuk az iraki és afganisztáni háború veszteségeit, a háború támogatottságát, elfogadottságát, nem nehéz összefüggést felfedeznünk a veszteségek növekedése és a háború elutasítottsága között. Beszédes adat például az alábbi két ábra:



1. ábra: Az ősz-áldozatok száma az adatfelvétel hónapjáig[2]

[1] Aszimmetrikus konfliktus alatt az olyan konfliktust értem, amelyben résztvevők között jelentős a technikai, katonai, társadalmi, gazdasági különbség.

[2] Forrás: Pew Research Center: Public Attitudes Toward the War in Iraq: 2003-2008, http://www.pewresearch.org/2008/03/19/public-attitudes-toward-the-war-in-iraq-20032008/ (Letöltés ideje: 2016. 10. 10.)



2. ábra: Szövetséges erők veszteségei[3]

Ezt felismerték napjaink egyéni vagy politikai célokból tevékenykedő terroristái is. Az ISIS[4] különösen hatékonyan alkalmazta, alkalmazza a közösségi média által nyújtott eszközöket propagandacélokra.[5]

A hatékony egészségügyi rendszer képes a veszteségek csökkentésére, fordított esetben pedig sajnálatos módon annak növelésére. A hatékony egészségügyi rendszer további előnye, hogy a nagy költség- és időigénnyel kiképzett katonáink hamarabb képesek visszatérni egy-egy sérülést követően a harcmezőre. A morális előny, illetve következmény is adott: ha megmentjük a hatékony egészségügyi rendszer révén a katonáink életét, ha életeket mentünk, akkor egész egyszerűen katonáink motiváltabbá válnak. A más életek megmentésnek előnyére csak egy, elsőre talán nem is egyértelmű példa: a szír polgárháború áldozatainak kezelése izraeli (katonai) kórházakban.[6]

Az aszimmetrikus konfliktusok kezelése során – különösen ha az a hátországban történik – speciális módon kell az egészségügyet üzemeltetnünk, működtetnünk. Ez a működési modell, ahogyan azt a hazai, vonatkozó jogszabályok és dokumentumok is nevezik, az egészségügyi válsághelyzeti működés Egészségügyi válsághelyzet pedig a jogszabályi definíciók (az egészségügyről szóló 1997. évi CLIV törtvény 228. §) szerint akkor következik be, amikor bármilyen okból kifolyólag az egészségügyi ellátási szükségletek, igények és a helyben

---

[3] Forrás: A „Coalition Military Fatalities By Year and Month" táblázat alapján http://icasualties.org/Iraq/index.aspx (Letöltés ideje: 2016. 10. 10.) készítette a szerző

[4] Iraki és Szíriai Iszlám Állam - Islamic State of Iraq and Syria

[5] KRIZBAI Diána Daniella: Az Iszlám Állam néven ismertté vált terrorszervezet "propagandagépezete", Hadtudomány (Online), 2015/25. (E-szám). pp. 285-295. http://real.mtak.hu/31158/1/24_KRIZBAI_DIANA_DANIELLA.pdf (Letöltés ideje: 2016. 10. 12.)

[6] Yoav ZITUN: Israel continues to save Syrian lives, http://www.ynetnews.com/articles/0,7340,L-4838412,00.html (Letöltés ideje: 2016. 10. 12.)

rendelkezésre álló kapacitás közötti súlyos aránytalanság következik be. Ilyen esetekben az ellátórendszer nem képes az addigi színvonalon ellátást nyújtani, valamennyi ellátandót – mindezt tág értelemben véve – megfelelően ellátni. Az egészségügyi válsághelyzet fontos további ismérve, hogy a helyzet felszámolása, illetve kezelése az egyes szereplők koordinált együttműködését követeli meg. Az addig megszokott színvonal teljesíthetetlensége döntően kapacitáshiány, illetve az ellátórendszer sérülése miatt kövezik be. Ezt az úgynevezett kompromisszumos medicina némileg kompenzálja, azonban az ilyen esetben történő ellátás az életminőséget esetlegesen nagymértékben befolyásolja.[7]

Az aszimmetrikus konfliktus természetéből eredő váratlanság, gyors lefolyás következtében a megítélésem szerint csak az előre felkészített vezető-irányító rendszer és szakszemélyzet, előre tartalékolt egészségügyi eszközök, és a naprakész, állandóan frissített tervek birtokában van reális esély az esemény egészségügyi következmények sikeres felszámolására. Ahogyan azt dr. Svéd László több értekezésében is kifejti, az egészségügyi válsághelyzetek felszámolásának tudománya, a katasztrófa-orvostan (ennek része a fentebb említett kompromisszumos medicina) az orvostudomány viszonylag új ága, amely a sürgősségi ellátás és katasztrófa-menedzsmentből alakult ki.[8] Ennek az az oka, hogy a nagyszámú, tömeges sérült ellátása, a járványhelyzet – egészségügyi válsághelyzet – felszámolása sok esetben illetve tekintetben már nem is orvos-szakmai, sokkal inkább szervezési, logisztikai kérdés. Az alapvető cél ugyanis a rendelkezésre álló eszközökkel minél több sérült megmentése (megfelelő szintű ellátása). E célnak alárendelve történik az ellátás megszervezése. Az ellátásszervezés a betegek osztályozása (triage) mentén történik, amely során a sérültek legnagyobb[9] csoportjának számító könnyű és közepes sérültekre fókuszál. Alapelv az is, hogy a sérültek osztályozását, amely kiemelt jelentőségű az esemény felszámolása során, és annak rendszeresen ismétlődnie szükséges, a legtapasztaltabb orvos – illetve szakdolgozó – kell, hogy végezze.[10]

Amíg az aszimmetrikus konfliktusban az ellenfél humán erőforrásai bőségesek, amíg ennek az erőforrásnak az "ára" (elvesztésére való érzékenység) alacsony, amíg ezek az emberek/felkelők/katonák/terroristák könnyen mobilizálhatók, motiválhatók, sőt, fanatizálhatók, a tradicionális fegyverek használta inkább előtérben marad. Sokkal inkább, mint a nagy anyagi ráfordítást, szervezeti hátteret,

---

[7] MAJOR László (2010): A katasztrófa-felszámolás egészségügyi alapjai, Semmelweis Kiadó és Multimédia Stúdió, Budapest, pp. 109-110.

[8] Dr. SVÉD László: A Magyar Honvédség egészségügyi biztosítása elvének és gyakorlatának változásai, sajátosságai, különös tekintettel a haderő átalakításra, a NATO-ba történő integrálásra, a különböző fegyveres konfliktusok, valamint a békefentartó, béketeremtő és -támogató tevékenységre, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, PhD értekezés, 2003.

[9] Az ún. 5x20 szabály szerint általában 20-40% könnyű, 20-40% közepes (mindösszesen 60 %) súlyos sérült 20%, illetve 20% rendkívül súlyos sérülttel számolhatunk. Lásd Dr. SVÉD László – Dr. VEKERDI Zoltán – Dr. SÓTÉR Andrea: Quo Vadis Honvédorvostan? in Hadtudományi Szemle, 2015. I. szám, pp. 359-380. Hasonló elvet követ a NATO Civil Emergency Planning Committee által kiadott dokumentum: „Guidance to National Authorities for Planning for Incidents Involving Catastrophic Mass Casualities" című, AC/98-D(2018)0002 számú dokumentum

[10] MAJOR László (2010): A katasztrófa-felszámolás egészségügyi alapjai, Semmelweis Kiadó és Multimédia Stúdió, Budapest, pp. 109-110.

és szervezést igénylő CBRN (vegyi, biológiai, radio-nukleáris) ágenseké. Az ellenség célja ugyanis a jelenlegi konfliktusos környezetben sokkal inkább elérhető tradicionális támadásokkal: a fegyver a feketepiacról viszonylag könnyedén beszerezhető - sőt, sok esetben még ez sem szükséges - a támadások előkészítésének rizikója, szervezeti háttér-igénye, logisztikai költsége sokkal alacsonyabb, mint bármely más ágensé. A közelmúltban teherautóval Európában elkövetett támadásokból legalábbis mindenképpen erre következtethetünk. Abban az esetben, ha ellenfél "hátországa", erőforrásai, illetve hosszú távú céljai változnak, ez szükségszerűen az eszközeit is megváltoztatja. A tokiói metróban 1995-ben az Aum Shinri Kyo (Legfőbb Igazság) szekta tagjai által elkövetett szaringáz-támadás, illetve a csoport egyéb működéséből is következtethetünk arra, hogy igenis számítanunk kell CBRN ágensekkel elkövetett támadásokra.[11]

Kérdéses, hogy akkor miért nem tapasztalunk több biológiai, vagy vegyi ágenssel elkövetett támadást, aszimmetrikus műveletet? Ennek okát részben már említettem korábban: a szervezeti, logisztikai, humán-erőforrás és költségoldal miatt mindezidáig olcsóbb volt tradicionális eszközökkel támadásokat végrehajtani.

További ilyen ok, hogy egész egyszerűen - szerencsénkre - nehéz megtalálni, illetve megalkotni az ideális bio-fegyvert, ami tárolása során stabil, könnyen legyártható, szállítható, de bevetéskor kellően hatásos, azaz nagy megbetegítő-képességgel bír, a potenciális fertőzést pedig nehéz kezelni, annak kimenetele halálos.

Egy 2015-ös nemzeti gyakorlat[12] egyik főszervezőjeként lehetőségem nyílt az általános reagáló képességet vizsgálni egy kellően kreatívan megalkotott, ugyanakkor a biológiai törvényeknek, a rendelkezésre álló technológiai-technikai ismereteiknek megfeleltethető ágenssel elkövetett bioterror-támadás következményeinek vizsgálatára. A gyakorlat során az elképzelések szerint 65 személyt menekítettek ki légi úton egy válságövezetből, akik közül 4 személy a hazaúton fertőző betegségek tüneteit mutatták. A gyakorlat célja annak vizsgálata volt, hogy a bioterror-támadásként, szándékosan, módosított majomherpesz vírussal fertőzött 4 fős csoport, illetve a többi utas kezelése, ellátása, elhelyezése hogyan zajlik, milyen végkimenetele lehet egy ilyen eseménynek. Annak ellenére, hogy a gép személyzetét és utasait - a nemzetközi jelzések jelentős hatására - szinte azonnal karanténba helyezték (karantenizálták), az egészségügyi szervek, a modellezés szerint járvány tört ki, amelyet csak nagyon komoly intézkedések meghozatala árán sikerült megfékezni.

Az információk megosztásának, időben történő rendelkezésre állásának kiemelt jelentősége van. Éppen ezért a civil közegészségügyi szervek számos olyan

---

[11] TAMÁSI Béla – FÖLDI László: A tokiói metróban végrehajtott szarin támadás katasztrófavédelmi aspektusai, Hadmérnök, 2011/3. pp. 68-78.

[12] CMX 15 gyakorlathoz kapcsolódó nemzeti gyakorlat dokumentációja: 1608/2015/EGP, az Emberi Erőforrások Minisztériumának belső használatú dokumentuma. A gyakorlat során külföldről hazánkba behurcolt fertőző megbetegedés miatt kialakult járványügyi helyzet kezelésére került sor. Ennek részeként 2015. március 6-án Pápán a NATO katonai attaséinak, illetve a hazai szakmai közönségnek bemutatásra került az Állami Egészségügyi Tartalék elemeiből az Egészségügyi Készletgazdálkodási Intézet által felállított Mobil Járványügyi Zárlat, amely ilyen formában egyedülálló Kelet-közép Európában, illetve hazánk tekintetében is egy új képesség.

információt, tudást, illetve technológiát birtokolnak, amelyek adott esetben kiemelt fontosságúak lehetnek egy aszimmetrikus konfliktus során. A korábban ismertetett gyakorlat eklatáns példája, hogy különösen a közegészségügyi események során az információk megosztása mennyire fontos lehet. Ilyen információforrás például a határokon átterjedő súlyos egészségügyi veszélyekről szóló 1082/2013/EU határozat[13] alapján működő korai figyelmeztető és gyorsreagáló rendszer[14], illetve a határozat alapján megosztott biológiai, vegyi, környezeti, illetve ismeretlen eredetű veszélyre vonatkozó információk. Az Egészségügyi Világszervezet (WHO) hasonló célú[15] rendszerével szintén napi szintű az információ-áramlás. Problémásnak látom ugyanakkor azt, hogy a civil és katonai szervek között nem kellően dinamikus az információ-megosztás.

Megítélésem szerint – ahogyan ezt egy korábbi kéziratomban is kifejtettem – a katonai egészségügynek – a civil egészségüggyel karöltve – az aszimmetrikus konfliktusokra való hatékonyabb felkészülés érdekében:

- fokoznia kell az egészségügyi hírszerző képességeit. A korai detektálás, előrejelzés, a gyors diagnosztika elengedhetetlen;
- fokoznia kell a (légi)evakuációs képességeit, azaz a sérültet még gyorsabban professzionális ellátóhelyre kell juttatnia;
- erősíteni szükséges a rehabilitációs képességeket. A rehabilitált, ugyanakkor komoly tapasztalatokkal rendelkező, a korábbiakban nagy forrás- és időigénnyel kiképzett katonák más beosztásban, de a szervezet segítségére válhatnak. Ez azonban hazánkban csak a civil egészségügyi szervekkel kooperálva képzelhető el;
- biztosítani kell a civil és katonai rendszerek közötti tudásmegosztás rendszerét, az információ-, illetve tapasztalatáramlást erősíteni kell.

A civil-katonai együttműködés szükségességét az egészségügy területén számos tényező indokolja:[16] A civil, és különösen a katonai egészségügyi szolgálatok kapacitása jelentős módon csökkent mind a meglévő, működő, mind pedig a tartalékkapacitások tekintetében. Ez magában hordozza, hogy egy esetleges egészségügyi válsághelyzet esetén önállóan, a másik támogatása nélkül nem képes kezelni a kialakult helyzetet. Mindkét oldalon léteznek hiányzó, vagy egymást kiegészítő ellátási, reagálási képességek. A humán erőforrások biztosítása mindkét rendszer számára kihívásként jelentkezik. A civil egészségügyi rendszereknek képesnek kell lennie a válsághelyzetek kezelésére, a normál működési rendből való gyors áttérésre.

---

[13] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013D1082&qid=1537448542343&from=EN (Letöltés ideje: 2018. 03. 20.)

[14] Early Warning and Response System (EWRS)

[15] WHO's Early Warning, Alert and Response System (EWARS) http://www.who.int/emergencies/kits/ewars/en/ (Letöltés ideje: 2018. 03. 21.)

[16] Lásd bővebben: dr. RADNÓTY Gábor: A civil-katonai együttműködés területei; In dr. KESZELY László (szerk.) Az átfogó megközelítés és a védelmi igazgatás; Budapest: HM Zrínyi Média Közhasznú Nonprofit Kft., 2013., pp. 111-147.

Annak érdekében, hogy az egészségügyi ellátórendszer az aszimmetrikus konfliktusokra kellő hatékonysággal rendelkezésre álljon, az alábbiakra van szüksége, amelyek gyakorlatilag az egészségbiztonság alapját is képezik:

- egészségügyi hírszerzés, mely a prevenció (pl. oltások) alapja,
- kiterjedt közegészségügyi ellátó-rendszer,
- élelmiszerbiztonság (biztonságos ivóvíz és élelmiszer),
- egészségügyi kimentési, illetve szállítási képesség,
- hatékony ellátás (modern eljárások, eszközök, gyógyszerek, terápia), és az ezt kiszolgáló modern logisztikai ellátórendszer (pl. gyógyszer-utánpótlás)
- rehabilitációs rendszer (pl. végtagpótlás),
- mentális segítségnyújtási rendszer.

A fentiek elérése érdekében kiemelt jelentőségű:

- Egységes vezetési, irányítási és koordinációs rendszert kiépíteni. Az aszimmetrikus támadást követően képesnek kell lenni a civil és egyéb (rendvédelmi) erők tevékenységének összehangolására, az alá-fölérendeletségi viszonyok konkrét, és gyors meghatározására. Az eltérő ellátási protokollokat – lehetőség szerint – össze kell hangolni, vagy a műveleti területek meghatározásakor figyelemmel kell lenni az eltérésekre;
- Biztosítani szükséges az ellátórendszer megfelelő bővíthetőségét, az egyéb erőforrások bevonásának szabályozott módját;
- Rendszeressé, szisztematikussá kell tenni az információ- és tapasztalat-megosztást a civil és katonai oldal között. Mindezt a képzési, továbbképzési rendszerben intézményesen kell megjeleníteni;
- Olyan jogi-igazgatási-szabályozási környezetet kell kiépíteni, mely a fenti célok hatékony végrehajtását biztosítja.

A fentiekből láthatjuk, hogy az egészségügy nagyon fontos szerepet tölt be az aszimmetrikus konfliktusok sikeres megvívásában: önmagában a jó egészségügyi rendszer nem elégséges a sikerhez, ugyanakkor egy rosszul szervezett egészségügyi rendszer fokozza, fokozhatja a sérülékenységünket, a konfliktust akár indokolatlan módon el is nyújthatja, vagy akár lehetővé teheti, hogy az ellenfél elérje stratégiai céljait. A várható kihívások megkövetelik, hogy az egészségügyre, az egészségügyi biztonságra sokkal hangsúlyosabban fordítsunk figyelmet.

Felhasznált irodalom:

- Az egészségbiztonság javítása. Európai Bizottság, 2014. http://ec.europa.eu/chafea/documents/health/hp-infosheets/health_security_informationsheet_hu.pdf (Letöltés ideje: 2017. 07. 25.)
- Pro-Qualy: Az egészségügyi ellátás minőségének komponensei. 2017. http://www.pro-qaly.hu/az-egeszsegugyi-ellatas-minosegenek-komponensei-88.html (Letöltés ideje: 2017. 07. 25.)
- Egészségügyi Fogalomtár https://fogalomtar.aeek.hu/index.php/Kezd%C5%91lap (Letöltés ideje: 2018. 08. 10.)
- SVÉD László szerk.: A katona-egészségügy, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009.
- BORDÁS Imre: Vegyi fegyverek. Budapest, Országos Kémiai Biztonsági Intézet, 2006.
- FALUDI Gábor: A vírusok és a bioterrorizmus. In. Berencsi György (szerk.): Orvosi molekuláris virológia. Convention Budapest Kft., Budapest, 2005.
- FALUDI Gábor: A biológiai fegyver és az ellene való védelem – biovédelem (orvosi) kérdései. PhD disszertáció, ZMNE KMDI, 2012.
- FALUDI Gábor et al.: A toxinok mint biológiai harcanyagok. Honvédorvos, 51. évf., 1999/4., pp. 192-210.
- FALUDI Gábor – RÓKUSZ László: A biológiai fegyver. Budapest, Magyar Honvédség Egészségügyi Csoportfőnökség, 2003.
- KRIZBAI Diána Daniella: Az Iszlám Állam néven ismertté vált terrorszervezet "propagandagépezete", Hadtudomány (Online), 2015/25. (E-szám). http://real.mtak.hu/31158/1/24_KRIZBAI_DIANA_DANIELLA.pdf, pp. 285-295. (Letöltés ideje: 2016. 10. 12.)
- MAJOR László (2010): A katasztrófa-felszámolás egészségügyi alapjai, Semmelweis Kiadó és Multimédia Stúdió, Budapest, pp. 109-110.
- dr. RADNÓTY Gábor: A civil-katonai együttműködés területei; In dr. KESZELY László (szerk.) Az átfogó megközelítés és a védelmi igazgatás; Budapest: HM Zrínyi Média Közhasznú Nonprofit Kft., 2013. pp. 111-147.
- SHAMIEH. Luna: Az „Iszlám Állam" kommunikációs stratégiája és taktikája, Nemzet és Biztonság, 2016/3. szám, pp. 18-41.
- Dr. SVÉD László: A Magyar Honvédség egészségügyi biztosítása elvének és gyakorlatának változásai, sajátosságai, különös tekintettel a haderő átalakításra, a NATO-ba történő integrálásra, a különböző fegyveres konfliktusok, valamint a békefentartó, béketeremtő és -támogató tevékenységre, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, PhD értekezés, 2003

- SVÉD László: A sérültellátás katasztrófa és katona-orvosi vonatkozásai. Honvédorvos, 57. évf. 2005/3-4., pp. 121-133.
- SVÉD László: A katona-egészségügy: A tervezéstől a műveletig. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009
- SVÉD László: A védelem-egészségtudomány kihívásai. Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata. 19. évf., 2009/3-4., pp. 28-30.
- SVÉD László – VEKERDI Zoltán: Algoritmusok a katasztrófa helyzetek egészségügyi biztosításához. Honvédorvos, 60. évf., 2008/1-2., pp. 16-26.
- Dr. SVÉD László – Dr. VEKERDI Zoltán – Dr. SÓTÉR Andrea: Quo Vadis Honvédorvostan? in Hadtudományi Szemle, 2015/1., pp. 359-380.
- TAMÁSI Béla – FÖLDI László: A tokiói metróban végrehajtott szarin támadás katasztrófavédelmi aspektusai, Hadmérnök, 2011/3. pp. 68-78.
- Yoav ZITUN: Israel continues to save Syrian lives, http://www.ynetnews.com/articles/0,7340,L-4838412,00.html (Letöltés ideje: 2016. 10. 12.)
- Az Egészségügyi Válsághelyzetek Kezelésének Országos Terve (2014)
- WHO's Early Warning, Alert and Response System (EWARS) http://www.who.int/emergencies/kits/ewars/en/ (Letöltés ideje: 2018. 03. 21.)
- https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013D1082&qid=1537448542343&from=EN (Letöltés ideje: 2018. 03. 20.)

CSURGÓ ATTILA

A KATONAI MŰSZAKI TÁMOGATÁS AZ ASZIMMETRIKUS HADVISELÉS KORÁBAN, KÜLÖNÖS TEKINTETTEL A RÖGTÖNZÖTT ROBBANÓSZERKEZETEK ELLENI HARCRA

"IEDs have been the predominant weapon of insurgents in the Iraq War and the Afghanistan War, [...], they will continue to be the weapon of choice for guerrillas and insurgents for the foreseeable future."
Peter MANSOOR[1]

Bevezetés

Az utóbbi években végrehajtott katonai műveletek tapasztalatait figyelembe véve a fegyveres küzdelem megvívása jelentős mértékben megváltozott mind formai, mind tartalmi szempontból. Több új jelenség fordult elő a katonai műveletek megvívásakor, különösen a békekikényszerítés, a békefenntartás, békeépítés és a felkelők elleni katonai műveletek alatt. A tapasztalatokat elemezve (ide értem saját műveleti területen szerzett tapasztalataimat is[2]) megállapítható, hogy a korszerű, technikailag jól felszerelt fegyveres erő nem az egyetlen feltétele a katonai műveletek sikeres végrehajtásának, a győzelemnek. Ugyan a katonai erő továbbra is az ellenség védtelenné tételéreés akaratának rákényszerítésére készül – ahogy azt Clausewitz írta – és annak eszköze maradt, de a tapasztalatok alapján napjainkban egyre több az olyan műveleti helyzet, amikor a katonai győzelem érdekében civil szervezetek tevékenységére is szükség van, sőt a békeépítését kell folytatni a hadszíntér egyes részein a katonai műveletek végrehajtásával egy időben. Írásomban nem kevesebbre vállalkozom, mint jelenkorunk hagyományostól eltérő hadviselési formájában az aszimmetrikus hadviselésen belül beazonosítsam a katonai műszaki támogatás feladatait. Mivel doktorandusz hallgatóként választott kutatási témám a műszaki támogatás kihívásai a 21. században, ezért fontosnak tartom, hogy egy szakcsapat, amelyhez magam is tartozom, ismerje helyét és szerepét, a 21. század hadviselésének egyik legjellemzőbb formájában, az aszimmetrikus hadviselésben. Ugyanakkor jelen írásomban nem célom, hogy beazonosítsam az összes lehetséges

[1] MANSOOR, Peter: Improvised Explosive Device, Weapon, In Encyclopedia Britannica, Forrás: https://www. britannica.com/technology/improvised-explosive-device (Letöltésideje: 2018. 05. 22)

[2] A balkáni válság stabilizációs feladatainak végrehajtására létrehozott erők kötelékében ellátott beosztásaim: (SFOR) 3 alkalommal: 1997-98. Magyar Műszaki Kontingens (MMK, Okucani) szakasz, majd századparancsnok, 2002-2003. SFOR HQ: műveletirányító törzs, műszaki főnökség, hadműveleti főtiszt majd hadműveleti főnök, végül 2004-ben az ideiglenesen újból megalakított MMK parancsnok helyettes. 2005-06-ban Albánia NATO csatlakozását előkészítő parancsnokság tanácsadói csoportjában (NATO HQ Tirana, NAT), műszaki tanácsadóként, 2011-ben a líbiai műveleteket vezető törzs (OperationUnifiedProtector, Lybia), összhaderőnemi műveleti központ, (JOC) váltásvezetőjeként tevékenykedtem.

műszaki támogatási formát, ezért - mint azt a kutatási témafelvetésemben[3] is tettem - szűkítem a vizsgált területet az IED-k[4] elleni harccal kapcsolatos támogatási feladatokra.

Az aszimmetrikus hadviselésről általában

Az aszimmetrikus hadviselés, vagy a hadviselés aszimmetrikus formája? Számos anyagot olvasva ez a kérdés fogalmazódott meg bennem. Szendy professzor úr a Hadelmélet és Katonai Műveletekcímű könyvének első kötetében a hadviselés formájaként írja le, majd példákkal bizonyítja, hogy a különböző történelmi korokban az aszimmetria folyamatosan jelen volt a hadviselésben[5]. A professzor úr megállapítása alapján a kérdésemre a válasz nem más, mint az aszimmetria, a hadviselés megvalósulási módja, velejáró jellemzője. Könyvében az aszimmetrikuságról szóló szakaszt a következő gondolatokkal zárja le: *„A hadviselés aszimmetrikusságának igazán érdekes és elemzésre érdemes iskolapéldája az eltérő hadikultúrák alapján szervezett és funkcionáltatotthaderők, fegyveres erők közötti fegyveres küzdelem*[6]*."* A hadikultúrák tanulmányozásához Forgács Balázs 2009-ben íródott PhD-értekezését[7] választottam, amely Kovács Jenőre[8] hivatkozva értelmezi a hadikultúrát: *„Olyan társadalmi és katonai szellemi és anyagi alapfeltétel, adottság, amelyre ráépülnek az aktuális háború jellegéből, a haditechnika színvonalából, a hadszíntér-viszonyokból, a moráltól függő alakzatok.[...]A hadikultúra a társadalmi élet egészét (tudomány, művészet, oktatás, gazdaság stb.)áthatja."*[9]Kovács Jenő a hadikultúrákat három területre osztja: „mozgáscentrikus, anyagcentrikus és gerilla hadviselés"[10]. A gerilla hadviselés, mint a háború jellege már Ágh Attila könyvében[11] is megjelenik, amelyben az 1945 utáni háborúkat, mint modern "kisháborúkat" elemezve kategorizálja őket. Természetesen látnunk kell, hogy könyve a hidegháború végéhez közeledve íródott, a nagyhatalmak szembenállása, új fejlesztésű fegyvereik és természetesen a háború megvívására kidolgozott elméletek tesztelése is a megvívott kisháborúk során valósult meg.

---

3 Az MH műszaki támogatásának lehetséges irányai a 21. században, az erők megóvása során, különös tekintettel az rögtönzött robbanószerkezetek elleni harcra. Témavezető: Dr. habil. KOVÁCS Tibor ny. mk. ezds.

4 Rögtönzött robbanó szerkezet angol fordítása: Improvised Explosive Device, angol kifejezés rövidítése

5 SZENDY István: Hadelmélet és Katonai Műveletek, I. kötet, A katonai műveletek elmélete és gyakorlata, Nemzeti Közszolgálati és Tankönyvkiadó, Budapest 2013. pp. 140-141. ISBN: 9786155344251

6 SZENDY i. m. p. 142.

7 FORGÁCS Balázs: Napjaink hadikultúrái (A hadviselés elmélete és fejlődési tendenciái a modern korban) PhD-értekezés, ZMNE-KLHK/HDI Budapest, 2009. Forrás: http://docplayer.hu/4930393-Napjaink-hadikulturai-a-hadviseles-elmelete-es-fejlodesi-tendenciai.html (Letöltés ideje: 2018. 05. 12.)

8 Kovács Jenő altábornagy (1929 - 1996) katonai vezető és teoretikus, fő műve a: Magyarország katonai stratégiája.(Komplex kutatási téma). I–III., Kézirat, Bp., 1993., 1995., 1996 In FORGÁCS Balázs: In memoriam Kovács Jenő, Hadtudomány 2009/1-2. sz. Forrás: http://mhtt.eu/hadtudomany/2009/1_2/105-112.pdf Letöltés ideje: 2018. 05. 24.

9 FORGÁCS(PhD-értekezés) p. 41.

10 Uo.p. 42.

11 ÁGH Attila: Konfliktusok háborúk, Zrínyi katonai, Budapest, 1989. p. 304. ISBN: 9633265924

Ágh Attila rendszere 4 típusú háborút (vagy konfliktust) különböztet meg[12]:

1. Az új konvencionális kisháború, amelynek okaként az időszakban létrejövő regionális középhatalmakat jelöli meg. Ezen típusú háborúkra a jellemző, hogy reguláris erők vívják, a korszerű haditechnikának döntő jelentősége van, illetve a felek stratégiát követnek, és a frontvonal, valamint a hátország jól elkülönül egymástól.
2. A nem konvencionális háború, amely kategória okaként annak elhúzódó jellegét jelöli meg, és bár a jellemzői között megtalálhatjuk a reguláris erőket és a stratégiát is, elhúzódó jellege miatt megjelenik a gerilla háború.
3. A destabilizációs háború, amelyben már a konfliktus jellegét a nem katonai eszközök alkalmazása jellemzi. Továbbra is elhúzódó háborúról beszélünk, de alapvetően az ellenálló felek közötti front nem létezik, továbbá szinte minden eszköz megengedett a társadalmi, gazdasági, politikai destabilizáció érdekében. Fontos, hogy a felek közötti jelentős katonai aszimmetria ellenére a konfliktus kimenetele változó volt.
4. Az utolsó kategóriát már nem is háborúként, hanem anómiás[13] konfliktusként azonosítja. Az összecsapások gyakorlatilag leszűkülnek ösztönös rendezetlen és váratlan politikai és/vagy fegyveres erőszakra. Az ilyen jellegű konfliktusok tulajdonságai között megtalálhatjuk az idegengyűlöletet, a vallási fanatizmust és nem utolsó sorban az etnikumok közötti ellentétet.

A fenti kategóriákban, már a nem konvencionális háborúk ismérvei között is megjelenik a gerilla háború,mint a hadikultúrák egyik formája, de a bevezetőmben megfogalmazott cél elérése érdekében jelen korunk összecsapásainak, talán mondhatom,anómiás konfliktusainak elemzése szükséges. Ahhoz, hogy megértsük az IED-k szerepét és az általuk mind több területre kifejtett hatásukat, az Afganisztánban, Irakban vagy Szíriában kialakult aszimmetrikus konfliktusok vizsgálatát tartom szükségesnek.

Talán már ezen fejezet elején értelmeznem kellett volna az aszimmetriát, de mivel korábban már említett célom elérése érdekében alapműként vettem Resperger István – Kiss Álmos Péter –Somkuti Bálint aszimmetrikus hadviselésről írott könyvét[14], ezt a fogalmat most tisztázom:

- Szimmetria: *"Azonosság, azonos alakúság, általában arányosság, rend az egyes részek között."*
- Aszimmetria: *"A szimmetria hiánya a részek között, vagy az egészben"*[15]

Mielőtt az aszimmetrikus hadviselés konkrét meghatározására rátérnék, pontosítani szeretném a terminológiát. Hiszen a könyv két szerzője Kiss Álmos

---

12 Uo. pp.178-190.

13 Anomosz – görög szó, jelentése: rendezetlen. Lásd: FORGÁCS Balázs előadása: A háború tipológiája, NKE-HDI, Budapest, 2017. 11. 21.

14 RESPERGER István –KISS Álmos Péter –SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással, Zrínyi kiadó, 2013. Budapest, p. 421 ISBN: 9789633277171

15 Uo. p. 23

Péter és Somkuti Bálint PhD[16] értekezésében, 4. generációs hadviselésként azonosítja a hadviselés ilyetén formáját. Kiss Álmos például utal a hadikultúrák Kovács Jenő féle felosztására, azonban kihangsúlyozza, hogy míg a korábbi háborúkban vagy az anyag- vagy a mozgáscentrikus hadviselés dominált és csak nyomokban jelent meg a gerilla hadviselés, addig *"a negyedik generációs hadviselés a gerilla hadikultúra dominanciájának kora, melyben a másik két hadikultúra másodlagos szerepet kap.*[17]*"* Somkuti értekezésében a gerilla háborúkról úgy nyilatkozik, hogy annak megjelenése ugyan akkorra tehető, mint a hadviselésé[18]. A könyv szerzői közötti nézetkülönbségekre egyébként már a bevezetőben utalnak. Azonban számomra az aszimmetrikus hadviselés könyvben meghatározott fogalma egyértelműsíti, hogy nem az elnevezés a fontos, hanem a fogalom és az abban rejlő összefüggések értelmezése, megértése.

Az aszimmetrikus hadviselés fogalma: „*Pontosan körvonalazott politikai célok érdekében folytatott, gyakran több szervezet ideológiai, vallási, etnikai közösségén alapuló katonai, és nem katonai műveleteket, eljárásokat és módszereket alkalmazó közvetlen és közvetett hatásokra építő és egymás hatásait felerősítő, a biztonság különböző dimenziónak területét veszélyeztető harcmodor, főként harcászati eljárás, melyek együttes hatásával kényszeríthetjük akaratunkat az ellenségre.*[19]*"*

Írásom mottójául választott idézet nyer értelmet a fenti fogalom alapján. Az IED mint a gerilla hadviselés egyik fegyvere, valójában a harcászati eljárások fegyvere, de az általa okozott eseményhez párosított "propaganda", "stratégia kommunikáció" segítségével nem egy alkalommal sikerült a gyengébb félnek akaratát az erősebbre kényszerítenie. Hazai példaként említhetném a 2008 ban, az ISAF[20]misszió magyar vezetésű PRT[21] tűzszerész csoportjában bekövetkezett eseményeket[22]. Külföldi példaként a 2004-ben Madridban bekövetkezett robbantások szolgálnak, amelyek a spanyolok iraki szerepvállalására voltak hatással[23]. Az iraki háborút tovább vizsgálva megállapítható, hogy korai szakaszában konvencionális háborúként zajlott, de a béke megszilárdítása már

---

16 KISS Álmos Péter: A negyedik generációs konfliktusok jellemzői és tapasztalatai, PhD-értekezés, ZMNE/KLHK/HDI, Budapest, 2011. (DOI azo.: 10.17625/NKE.2012.011), SOMKUTI Bálint: A negyedik generációs hadviselés - az érdekérvényesítés új lehetőségei PhD-értekezés, ZMNE/KLHK/HDI, Budapest, 2012. (DOI azo.: 10.17625/NKE.2012.019)

17 KISS(PhD értekezés) p. 13.

18 SOMKUTI(PhD értekezés) p. 16

19 RESPERGER–KISS– SOMKUTIi. m. p. 23.

20 Nemzetközi Biztonsági Közreműködő Erő – International SecurityAssistanceForce angol kifejezés rövidítése

21 Tartományi Újjáépítési Csoport –ProvincialReconstruction Team angol kifejezés rövidítése

22 A PRT-4 váltás tűzszerész csoportban bekövetkezett események, amely 2008. 06. 10-én Kovács Gyula ftőrm (posztumusz hadnagy), majd 2008. 07. 12. Nemes Krisztián szds. (posztumusz őrnagy) halálához vezetett. A balesetek bekövetkezését követően a magyar vezetésű PRT tűzszerész tevékenysége korlátozásra került.

23 2004. március 11-én 13 IED robbant 4 vonaton, megölve 191 és megsebesítve 1800 embert. A támadás mögött az al-Kaida vonzáskörében álló terrorcsoport állhatott, mely így tiltakozott az ellen, hogy Spanyolország támogatta az Egyesült Államokat az iraki háborúban. Forrás: https://hu.euronews.com/2017/03/11/13-eve-tortent-a-madridi-terrortamadas (Letöltés ideje: 2018. 05. 12)

elhúzódó folyamat volt. Az IED-k tekintetében gyakorlatilag az iraki háború egy lépcsőfoknak tekinthető. Megjelennek az IED-gyárak[24].

Az rögtönzött robbanószerkezetről általában

Az IED mint kifejezés először a brit katonai körökben jelent meg az IRA[25] által különféle módon házilag barkácsolt robbanószerkezetek elnevezésére. Napjainkban, hogy megértsük mi is az IED, pontosabban milyen fenyegetést jelent a műveletet végrehajtó csapatokra, Michael Barbero altábornagy, a Joint IED Defeat Organization[26] (JIEDDO) igazgatója által megfogalmazottak az irányadóak: *"In the 20th century, artillery was the greatest producer of troop casualties. The IED is the artillery of the 21st century."*,azaz: műveleteket végrehajtó csapatoknál, a pusztítás mértékét figyelembe véve, míg a 20. században a tüzérség okozta a legnagyobb veszteségeket, most, a 21. században az IED vált a legpusztítóbb tűzfegyverré. Ugyanakkor az IED-k hazai terminológia értelmezése:„házilag készített robbanószerkezet" estenként tévútra vezethet, hiszen alapvetően egy olyan „bombakészítő" jelenik meg a szemünk előtt (virtuálisan), aki a kereskedelmi forgalomban beszerezhető anyagokból, az interneten elérhető leírások alapján eszkábál össze egy csőbombát, ritkán komolyabb szerkezetet. Nos, az Egyesült Államok vezette koalíciós erők által 2003 március 20. és május 1. között vívott iraki háború után, a kialakult biztonsági vákumban, a fegyver- és lőszerraktárak kiürítésre kerültek, sajnos általában nem a koalíciós erők által. Továbbá az iraki fegyveres erők feloszlatásával kiképzett, felkészített bombaszakértők kerültek a munkaerőpiacra, amely a bombagyárak megjelenéséhez vezetett[27]. Tehát minden adott volt, hogy a katonai eredetű lőszerek felhasználásával, akárcsak bennük lévő robbanóanyag kinyerésével, rendkívül pusztító IED-kat készítsenek.

2015-ben a Magyar Honvédség újdörögdi gyakorlóterén (rom)városi környezetben az 1. Honvéd Tűzszerész és Hadihajós Ezred (1. HTHE) tűzszerészei vezetésemmel bemutatták egy 82 mm-es aknavetőgránát (1. ábra) IED-ként kifejtett hatását. A gránát nem több mint 3,5 kg tömegű, a benne található robbanóanyag mennyisége kevesebb mint 40 dkg, a hatása mégis figyelemreméltó. A robbanás repeszhatása 25 m-es körben súlyos életveszélyes sérüléseket okozott az imitációs célanyagban, még a második emeleti ablakokban elhelyezett célanyagban is több repeszt találtunk.

---

24 SOMKUTI(PhD értekezés) p 85.

25 IrishRepublicanArmy – Ír Köztársasági Hadsereg

26 Összhaderőnemi szervezet az IED elleni harcra, amelyet az Egyesült Államok VédelmiMinisztériuma által 2006-ban létrehozott szervezet a DefenceTreatReductionAgency-n – Védelmi Ügynökség a Fenyegetések Csökkentésére – belül müködik. Forrás: https://www.jieddo.mil/ (Letöltés ideje: 2018. 05. 12.)

27 RESPERGER István előadása: Generációk a hadviselésben, aszimmetrikus hadviselés NKE/HDI Budapest, 2018. 05. 08.

2. ábra: 82 mm-s szovjet 6 szárnyú repesz aknagránát[28]

A feladat végrehajtásáról a HM Zrínyi Kht. filmet készített, amely a tűzszerész alakulat történetét feldolgozó könyv[29] DVD mellékleteként elérhető.

Az IED az aszimmetrikus hadviselés fegyvere

Hogy hogyan illeszkedik az IED az aszimmetrikus hadviselésbe, az eddig leírtakból levont következtetések, valamint a Combat Engineer 2017[30] és a Military Engineering 2018 konferenciákon[31] elhangzottak alapján az alábbiak szerint foglalom össze:

[28] Forrás: https://pyrocenter.hu/tuzijatek/galeria/showimage.php?image=2483 (Letöltés ideje: 2018. 05. 12.)

[29] BUCSÁK Mihály et al.:70 év az életveszély árnyékában – A magyar tűzszerész- és aknakutató alakulatok története 1945-2015. Zrínyi kiadó, Budapest 2015. ISBN: 9789633276532

[30] CombatEngineerConference (CE-17)2017. 11. 07-09. Nürnberg,

[31] Military EngineeringConference (ME-18) 2018. 02. 27-03. 01. London

3. ábra: Az aszimmetrikus hadviselés kialakulása
(saját szerkesztés)

Resperger István a „*Stratégiák és fogalmak háborúja, az aszimmetrikus hadviselés hadtudományi megközelítése"* című publikációjában[32]ábrákkal szemlélteti azokat az "indikátorokat", amelyekkel rávilágít a hadtudomány területén jelentkező eltérésekre. Az általam szerkesztett ábrával az IED helyét szerepét kívánom megtalálni a hadviselés ezen formájában. Az általam alapműként kezelt könyv 24. oldalán a szerzők is úgy fogalmaznak, hogy a „gyengébb" technikai fejlettségi szinten lévő fél az egyszerűen végrehajtható műveletek széles tárházát használja céljai elérése érdekében. A következő ábrán az aszimmetrikus hadviselés szabályainak jellemzőit foglalom össze.

[32] RESPERGER István: Stratégiák és fogalmak háborúja, az aszimmetrikus hadviselés hadtudományi megközelítése, Hadtudomány 2016/E., http://mhtt.eu/hadtudomany/2016/2016_elektronikus/4_resperger%20istvan.pdf, pp 38-43. (Letöltés ideje: 2018. 05. 12.)

4. ábra: Az aszimmetria szabályai
(saját szerkesztés)

Mindezek alapján általam levont következtetéseket a következő ábrával szemléltetem, illetve pontosítom mit is értek az IED fegyverként történő használatán.

5. ábra: Az IED az aszimmetrikus hadviselés fegyvere
(saját szerkesztés)

John Matthewsezds.(UK. A)[33] a ME-18 konferencián úgy jellemezte az IED elleni fejlődés szükségességét, hogy azt a folyamatosan növekvő fenyegetés vezérli. *(„Threat driven C-IED capability development”*). Ugyanakkor nyomatékosította, hogy szorosabb együttműködésre van szükség a fegyvernemek és szakcsapatok, a felderítéssel foglalkozó ügynökségek és a civil szféra között az IED elleni védelem területén. A következőkben megvizsgálom, hogy az IED-k jelentette fenyegetés hogyan jelentkezik a műszaki támogatásban.

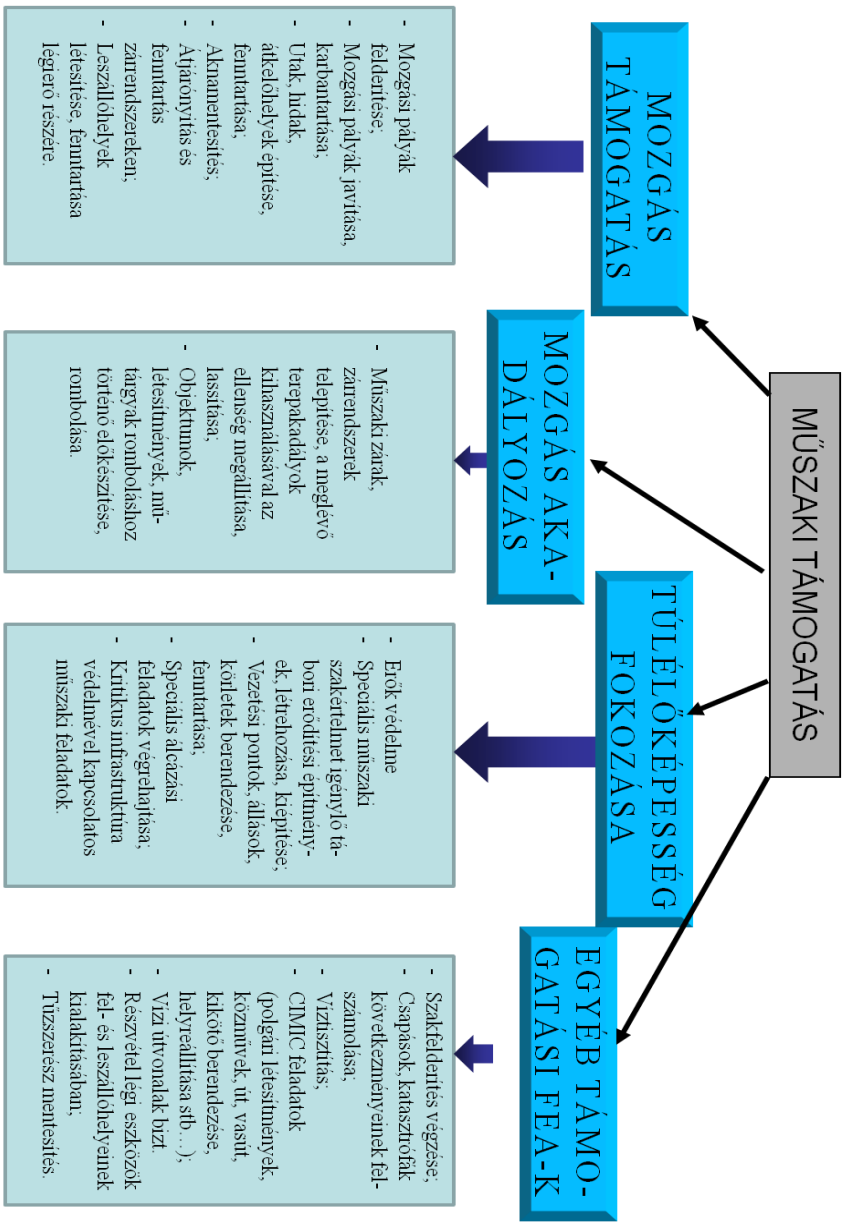
Az IED hatása a műszaki támogatásra

A műszaki támogatás – amint arra már bevezetőmben is utaltam – nem a műszaki csapatok öncélú tevékenysége a harc megvívása során, hanem a művelettámogatás fajtája. Fogalmát tekintve Szabó Sándor – a Magyar Hadtudományi Társaság (MHTT) műszaki szakosztály elnöke sajnálatos haláláig – által meghatározottakat veszem alapul: *„A műszaki támogatás mindazon speciális tevékenységek és rendszabályok összessége, melyeket az V. cikkely szerinti (harc, hadművelet), illetve az V. cikkely hatálya alá nem eső (válságreagáló) műveletek előkészítése és végrehajtása során műszaki feltételként meg kell teremteni a feladatot végrehajtó csapatok tevékenységének sikeres megvalósításához.”*[34] A műszaki támogatás feladatrendszere 4 fő területre összpontosul, amelyet a NATO STANAG 2394[35] alapján a következő ábrában foglalok össze.

[33] DefenceExplosiveOrdnanceDisposal, Munitions and SearchTraining Regiment – a britVédelmiMinisztérium alárendeltségében lévő tűzszerész felkészítésért felelős ezred parancsnokhelyettese

[34] SZABÓ Sándor: A műszaki támogatás cél - és feladatrendszerének változása az I. világháború végéig. In. Műszaki Katonai Közlöny (online kiadvány) XXIV. évf. 2. szám 2014. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2014_2sz/1_A%20muszaki%20tamogatas%20cel-%20es.pdf, p. 2 (Letöltés ideje: 2018. 05. 12.)

[35] AlliedJointPublication AJP- 3.12, Edition 3, version 1, STANAG 2394 Szövetséges Katonai Műszaki Harcászati Doktrína, AlliedTacticalDoctrinefor Military Engineering. NATO Standardization Office (NSO) kiadványa: 2013. 05. 02. 128 old. Magyarországi hatályba léptetés: 168/2015 (HK.5) MH ÖHP intézkedés. Forrás: http://www.kozlonyok .hu/kozlonyok/Kozlonyok/13/PDF/2015/5.pdf (Letöltés ideje: 2018. 05. 12.)



6. ábra: A műszaki támogatás területei[36]
(saját szerkesztés a STANAG 2394 alapján)

Megítélésem szerint az IED-k jelentette fenyegetésre, kihívásokra adandó válaszok nem egy új területe a műszaki támogatásnak, hanem a területeken belül kell beazonosítanom a feladatokat. Természetesen a tűzszerész feladatok a műszaki támogatás minden területén megjelennek, legyen az katonai eredetű

[36] Uo.

robbanószerkezetek eltávolítása (EOD[37]), vagy az rögtönzött eszközök eltávolítása (IEDD[38]), de akár a robbanószerkezetek felderítését (EOR[39]) is ide kell sorolnom. Azt hiszem nem kell hangsúlyoznom a háborúk utáni tűzszerész mentesítés fontosságát, legyen az Afganisztán, Irak, vagy akár honi terület. Több mint 70 évvel a II. világháború után évente több mint 2000 bejelentés érkezik az 1. HTHE tűzszerész ügyeletére. Az újdörögdi gyakorlótéren felrobbantott gránát is a mentesítés során került elő, amelyet 1943-ban gyártottak. Tehát a tűzszerészek az IED elleni harcban fontos szerepet játszanak, így a területek vizsgálata során ezen feladatokat külön nem részletezem.

1. Mozgástámogatás, azaz a műveleteket végrehajtó csapatok mozgásának támogatása:
Az iraki és afganisztáni műveleti területeken a szövetséges erők mozgásának támogatása érdekében jelent meg a Route Clearance Team (RCT), azaz a magyar terminológiában útfelderítő- és mentesítő képesség. Bár 2014-ben az 5. Dandár[40] műszaki zászlóaljának bázisán kialakításra került egyfajta kezdetleges képesség. A csoport a robbanó szerkezetek felderítésére, csak kézi eszközökkel illetve, a Magyar Honvédségben 1970-es években rendszeresített UAZ-469 terepjáró személygépkocsira szerelt, indukciós elven működő, alapvetően aknakereső járművel rendelkezik, ezért a robbanó eszközök eredményes felderítése érdekében, további fejlesztések szükségesek hazai viszonylatban.

2. Mozgás akadályozás, azaz az ellenség mozgásának akadályozása:
A műszaki zárrendszerek telepítése a műszaki csapatok létével egyidős, amelynek egyik klasszikus formája a robbanó műszaki zárak, zárrendszerek, valamint az aknamezők létesítése, kiépítése. T. P. McGuire vezérőrnagy[41] (Az Európában állomásozó amerikai csapatok parancsnok helyettese) a CE-17 konferencia megnyitójában rámutatott, hogy a szövetség (főleg az európai szövetségesek)aknatelepítő képességei nem kielégítőek. Az MH-ban gyakorlatilag kisebb számmal rendelkezünk ezen képességgel. Ugyanakkor a rendelkezésünkre álló tüzérségi lőszerek felhasználásával a nem robbanó műszaki zárakat ki tudjuk egészíteni, azaz az IED-kat saját céljainkra is használhatjuk, amennyiben szükséges.

3. Túlélőképesség fokozása, azaz az erők védelmével kapcsolatos támogatási feladatok
A katonai táborok IED elleni védelmével kapcsolatosan két angol kifejezésre hívnám fel a figyelmet:„resilience” – rugalmasság, illetve a „stand-off distance” – a robbanások hatásainak elkerülése érdekében kialakított biztonsági távolság.
Rugalmasság alatt az erők olyan képességét értem, amely biztosítja a támadásokkal szembeni ellenállást, ugyanakkor képes gyorsan visszaszerezni az ellenálló képességét az ellenség behatása után. Az IED-k okozta meglepetést, a robbanást követő káoszt ellensúlyozandó képesség. A létesítmények, táborok kialakításának fontos eleme a biztonsági zónák kialakítása, azok műszaki berendezése a

[37] Explosive Ordenance Disposal– lőszermentesítés
[38] Improvised Explosive Device Disposal – rögtönzött eszközök eltávolítása
[39] Explosive Ordenance Reconnaissance –lőszerek felderítése
[40] Magyar Honvédség 5. Bocskai István Lövészdandár
[41] TimothyMcGuire vezérőrnagy 2016. 06. 01-től tölti be a United States Army Europe, Az Amerikai Egyesült Államok Európai Erőinek, parancsnokhelyettesi beosztását: Forrás: http://www.eur.army.mil/leaders/ (Letöltés ideje: 2018. 05. 27.)

rendelkezésre álló anyagokkal. A terület jelenleg szabályozatlan a Magyar Honvédségnél.
A „stand-off distance" meghatározása a robbanások hatásainak csökkentése érdekében szintén a területen jártas, műszaki szakember feladata. A szabályozatlanság hiányára Kiss Álmos Péter korábbi írásában[42] is utal.

4. Egyéb műszaki támogatási feladatokként azonosítottam minden olyan feladatot, amely nem része az első három területnek, összhangban a STANAG 2394-el, amely általános támogatásként azonosítja ezt a területet.
A műszaki támogatás ezen területén a CIMIC[43], civil katonai együttműködés keretein belül végzett támogatási feladatokat emelném ki. A hadszíntereken, az IED-k elleni védekezés területén szerzett tapasztalatokat lehet alkalmazni akár honi területeken is. Hazai viszonylatban példaként említeném a 2017- ben Budapesten megrendezett FINA 2017[44] rendezvény biztosítását, ahol több más katonai szervezet mellett már az MH 1. HTHE is bevonásra került.

Összegzés

A bevezetőmben utaltam arra, hogy a műszaki támogatás – az IED jelentette kihívások tükrében – újszerű feladatait keresem. Nem célom új támogatási terület beazonosítása, de meglévő területeken belül meggyőződésem, hogy új feladatok jelentek meg.
Meghatároztam az IED-k jelentette fenyegetés és az aszimmetrikus hadviselés kapcsolatát, az ebből levont következtetések egyértelműek számomra, azaz egy új fegyver megjelenése – bár esetünkben egy korábban ismert fegyver tömeges és gyorsan fejlődő alkalmazásáról beszélünk – hatással van a harc megvívására és annak mindenoldalú támogatására is. Értelmeztem a „Route Clearance" útfelderítő- és mentesítő képesség megjelenését, rámutattam az új fogalmak: „resilience" - rugalmasság, „stand- off distance" – a robbanások hatásainak elkerülése érdekében kialakított biztonsági távolság, megjelenésére. Értelmeztem az hazai terminológiában „házi készítésű robbanószerkezet" és a katonai eszközök felhasználásával készített IED-k közötti különbséget, figyelemmel a katonai eredetű lőszerekből készített IED-k pusztító hatásaira.

Mindezek alapján megállapítható, hogy az IED-k jelentette fenyegetés hatással van a műszaki támogatás feladataira.

---

42 Kiss Álmos Péter: Ahol a hadmérnök és a polgár találkoznak: a nemkritikus infrastruktúra műszaki védelmének szabályai és előírásai, In Hadtudomány elektronikus szám 2012. http://mhtt.eu/hadtudomany/2011/2011_elektronikus/2011_e_8.pdf, p. 7. (Letöltés ideje: 2018. 05. 14.)

43 Civil Military Cooperationangol kifejezés rövidítése

44 FederationInternationale de Natation, nemzetközi úszószövetség, budapesti rendezvénye 2017. 07. 14-30. között. Forrás: http://www.fina.org/content/17th-fina-world-championships (Letöltés ideje: 2018. 05. 27.)

Felhasznált irodalom:

- AlliedJointPublication AJP- 3.12, Edition 3, version 1, STANAG 2394 Szövetséges Katonai Műszaki Harcászati Doktrína, AlliedTacticalDoctrinefor Military Engineering. NATO Standardization Office (NSO) kiadványa: 2013. 05. 02. 128 old. Magyarországi hatályba léptetés: 168/2015 (HK.5) MH ÖHP intézkedés. Forrás: http://www.kozlonyok .hu/kozlonyok/Kozlonyok/13/PDF/2015/5.pdf (Letöltés ideje: 2018. 05. 12.)
- Ágh Attila: Konfliktusok háborúk, Zrínyi katonai, 1989. Budapest, p. 304. ISBN: 9633265924
- Bucsák Mihály et al.: 70 év az életveszély árnyékában; A Magyar Tűzszerész- és Aknakutató Alakulatok Története 1945–2015. Megfelelés a jelenkor kihívásainak (DVD melléklet) Budapest, MH Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft. 2015. ISBN 9789633276532
- Csurgó Attila: A forceprotection, az erők megóvásának alapjai, MKK online XXVIII. évf. 2018. 1. szám pp. 209-217.
- Forgács Balázs: Napjaink hadikulturái (A hadviselés elmélete és fejlődési tendenciái a modern korban) PhD értekezés ZMNE- KLHK/HDI Budapest, 2009. http://docplayer.hu/4930393-Napjaink-hadikulturai-a-hadviseles-elmelete-es-fejlodesi-tendenciai.html (Letöltés ideje: 2018. 05. 12)
- Forgács Balázs: In memoriam Kovács Jenő, Hadtudomány 2009/1-2. sz. http://mhtt.eu/ hadtudomany/2009/1_2/105-112.pdf (Letöltés ideje: 2018. 05. 24.)
- Jan MAZAL: The currenttendencywithinthe NATO policy in thearea of military engineering, engineerintelligence and forceprotectionimplications. MKK online XXII. évf. 2012. különszám pp. 110-124.
- KISS Álmos Péter: A negyedik generációs konfliktusok jellemzői és tapasztalatai. PhD értekezés, ZMNE/KLHK/HDI, Budapest, 2011. (DOI azo.: 10.17625/NKE.2012.011)
- KISS Álmos Péter: Ahol a hadmérnök és a polgár találkoznak: a nemkritikus infrastruktúra műszaki védelmének szabályai és előírásai, In Hadtudomány elektronikus szám 2012. http://mhtt.eu/hadtudomany/2011/2011_elektronikus/2011_e_8.pdf, p. 7. (Letöltés dátuma: 2018.05.14.)
- KOVÁCS TIBOR: Példák a katonai táborok biztonsági rendszereinek kialakítására, különös tekintettel a robbantásos merényletek megelőzésére, azok hatásai csökkentésére, Tanulmány: TÁMOP-4.2.1.B-11/2/KMR Robbantásos építményvédelem, kiemelt kutatási terület. p. 31. (2013)
- MANSOOR, Peter: Improvised Explosive Device, Weapon, In Encyclopedia Britannica, https://www. britannica.com/technology/improvised-explosive-device (Letöltésideje: 2018. 05. 22.)
- RESPERGER István –KISS Álmos Péter –SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással, Zrínyi kiadó. 2013. Budapest, p. 421. ISBN: 9789633277171

- RESPERGER István: Stratégiák és fogalmak háborúja, az aszimmetrikus hadviselés hadtudományi megközelítése, Hadtudomány 2016/E., http://mhtt.eu/hadtudomany/2016/2016_elektronikus/4_resperger%20istvan.pdf, pp 38-43.
- SOMKUTI Bálint: A negyedik generációs hadviselés – az érdekérvényesítés új lehetőségei, PhD értekezés, ZMNE/KLHK/HDI, Budapest 2012. (DOI azo.: 10.17625/NKE.2012.019)
- SZABÓ Sándor: A műszaki támogatás cél - és feladatrendszerének változása az I. világháború végéig. In. Műszaki Katonai Közlöny (online kiadvány) XXIV. évf. 2. szám 2014. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2014_2sz/1_A%20muszaki%20tamogatas%20cel-%20es_.pdf (Letöltés ideje: 2018. 05. 12.)
- SZENDY István: Hadelmélet és Katonai Műveletek, I. kötet, A katonai műveletek elmélete és gyakorlata, Nemzeti Közszolgálati és Tankönyv kiadó Budapest, 2013. ISBN: 9786155344251
- CombatEngineer 2017. konferencia (szervező: TDN.UK: http://combat-engineer.com/) 2017. 11. 07-09. Nürnberg (Németo.)
- Military Engineering 2018. konferencia (szervező: Defence IQ: https://militaryengineering .iqpc.co.uk/) 2018. 02. 28-03. 01.
- https://www.jieddo.mil/ (Letöltés ideje: 2018. 05. 12.)
- http://www.fina.org/content/17th-fina-world-championships (Letöltés ideje: 2018. 05. 27.)

DR. KASSAI KÁROLY – NAGYSZEGI TERÉZ – POZDERKA GÁBOR

STRATÉGIAI SZINTŰ KIBERVÉDELMI ÁTTEKINTÉS

Bevezetés

A 2016 júliusi varsói NATO-csúcstalálkozó alkalmával elfogadott Kibervédelmi Kötelezettségvállalás[1] (Cyber Pledge) végrehajtását értékelő első konferencia francia rendezésben történt 2018. május 15-én, Párizsban.

A hagyományteremtő szándékkal megrendezett esemény fő célja, hogy a NATO júliusi brüsszeli csúcstalálkozójának közeledtével *ráirányítsa a politikai döntéshozók figyelmét a kibervédelem kiemelt fontosságára*. Ennek jegyében a rendezvényre a tagállamok kibervédelmi szakértői mellett meghívottak voltak a NATO-nagykövetek is.

Az egynapos konferencia két fő részre tagolódott: délelőtt – a tagállamok NATO-nagyköveteinek részvétele mellett – magas szintű kerekasztal-beszélgetésekre került sor, míg délután szakértői workshopokat tartottak. A rendezvényt a házigazda Francia Köztársaság védelmi minisztere, Florence Parly és Jens Stoltenberg NATO-főtitkár nyitották meg.

Vezetői gondolatok

A francia védelmi miniszter megnyitó beszédében elmondta, hogy hazája kiemelten kezeli a kibervédelem kérdését és ezen a területen a Szövetségen belül is vezető szerepet kíván játszani.

Napjainkban a fenyegetések változnak, nem csak a felismerhető állami vagy katonai erő formájában jelennek meg. A kibertéri fenyegetésnek „nincs arca", nem ismerhetők fel a motivációk, az országok szállítási, védelmi rendszereire vagy a lakosságra is irányulhatnak. *Csak remélni lehet, hogy mindenki tudatában van a fenyegetéseknek*. A szövetségi keretek kapcsán a *legnagyobb kihívás a közös, összehangolt fellépés* a kibertérben (governance). A szövetségi-nemzeti koordináció nem köthető minisztériumhoz, minden szektorban azonosíthatók teendők. A katonai-civil együttműködés kiemelt fontosságú, ahol a folyamatosságra kell hangsúlyt fektetni, a „leggyengébb láncszem" elv miatt.

A kibertérből érkező fenyegetésekre adandó francia válaszokat ismertetve kiemelte, hogy a francia kormány minden szükséges eszközt igyekszik biztosítani az ország kibervédelmének megerősítéséhez, illetve a kibervédelem területén széles körű összkormányzati koordinációt valósítanak meg. A minisztériumok feladata, hogy a szakértők, az ipar és az oktatási intézmények (akadémiák) számára „hidakat építsenek ki" az együttműködés támogatása érdekében.

[1] NATO Warsaw Summit Communiqué 2016. 07. 08-09., https://www.nato.int/cps/ic/natohq/official_texts_133169.htm, p. 71. (Letöltés ideje: 2018. 09. 24.)

A hatékony kibervédelem *új eszközök és eljárások* alkalmazásában, a *kutatás és fejlesztés* támogatásában, a *jogi háttér* kialakításában és a *pénzügyi, humán feltételek* biztosításában keresendő.

A nemzeteknek meg kell érteni az együttműködés fontosságát bilaterális, NATO és EU szinteken. A Szövetség a kollektív védelem támogatását biztosítja, de a sokszor idézett 5. cikk mellett (kollektív védelem) nem szabad elfelejtkezni a 3. cikkről (önvédelmi feladatok) sem. A Szövetség a NATO rendszereknél szükséges ellenálló képesség (resilience) mellett a képzésre és a műveleti támogatásra koncentrál. A képzés részeként a kibervédelmi gyakorlatok a különböző szereplők együttműködésének gyakoroltatását, az interoperabilitás támogatását és az együttműködést szolgálják. A műveleti gondolkodás alapja, hogy naivitás abban hinni, hogy az ellenfél nem támad. A szövetségi katonai műveletek támogatása érdekében *a nemzetek által felajánlott kibertér hatásokra (cyber effect) van szükség*, mert robosztus, erős ellenféllel szemben komplex képességek szükségesek.

A NATO szerepéről szólva méltatta a Kibervédelmi Kötelezettségvállalást, amely véleménye szerint kiváló eszközt jelent a nemzeti erőfeszítések megsokszorozására.

A NATO-főtitkár az amerikai elnökválasztás során tapasztalt jelenségekkel, illetve a brit kórházaknál markánsan jelentkező kampánnyal (WannaCry) utalt az új kibertéri fenyegetésekre. A támadások esetében jelenleg megválaszolandó kérdés a támadó kibenléte, ködben zajlanak az események („fog on war"). A kibertérben történő támadások (cyber attacks) a napi élet részévé váltak, az egyre bonyolultabb szoftverek alkalmazása új támadási lehetőségeket nyújt („soft war"). Katonai területen mondható, hogy a jól látható, „harckocsival történő műveletek" mellett megjelentek a kibertér műveletek, *a kibertér kiemelt szerepet kap a műveletekben („core part of operations")*. Ezen műveletek sikeres végrehajtásához szükséges eljárásrendek és képességek azonosítása folyamatos, a kialakítás közös gondolkodást igényel a Szövetség tagjainak részéről.

A főtitkár a Szövetség kibervédelem területén játszott szerepéről adott áttekintést. A Szövetség az alábbi három területen tölt be kulcsfontosságú szerepet a kibervédelem tekintetében:

- támogatja az információmegosztást (information sharing);
- oktatási és képzési segítséget nyújt és
- biztosítja a szövetségi hálózatok védelmét.

A Pledge összetett hatású, a nemzeteket a többfajta megoldás megismerési lehetőségével segíti. Az információmegosztáson túlmenően a Szövetség kibertér műveleti parancsnokságot állít fel a kibertér-műveletek katonai műveletekbe történő integrálásának támogatása érdekében. A gyorsreagálású csoportok segíthetik a nemzeteket. A NATO Kibervédelmi Kiválósági Központ (NATO CCD COE) oktatási és képzési szerepe kiemelkedő, melyre jó példa, hogy az áprilisi Locked Shields nemzetközi kibervédelmi gyakorlaton már ezer fő vett részt.[2]

A Szövetség esetében *az elrettentés (deterrence)* kiemelkedő fontosságú. A lényeg egyszerűen vázolható: *a támadásnak drágának kell lennie, míg a védelemnek olcsóbbá kell válnia* (beleértve a műveletek tervezését és a várható

[2] More than 1000 cyber experts from 30 nations took part in Locked Shileds, https://ccdcoe.org/more-1000-cyber-experts-30-nations-took-part-locked-shields.html, (Letöltés ideje: 2018. 09. 24.)

következményeket) – beleértve a hagyományos katonai és a kibertér-műveletek kiegyensúlyozott alkalmazását.[3] E területen hangsúlyos követelmény, hogy *a Szövetségi műveleteknek a nemzetközi jogi normák szerint kell történnie a jövőben is*.

A kollektív védelem elvének alkalmazása (Észak-atlanti Szerződés 5. cikk), az ehhez szükséges körülmények azonosítása még nyitott kérdés, világos iránymutatás még nem adható (*„we will see"*). A kibertámadásra adandó válaszok – a támadás természetétől és következményeitől függően – széles skálát foghatnak át: *a diplomáciai és gazdasági szankcióktól kezdve a kibertérben megvalósuló válaszokon át egészen a hagyományos erők alkalmazásáig.*

A rendszerek védelmét újra kell gondolni, de e területen nem szabad elfelejteni, hogy a felhasználók viselkedése gyengítheti a védelmet.

Összefoglalásként elmondható, hogy a NATO 2016-os Varsói Csúcstalálkozó kibertér-műveletekre vonatkozó irányelvei mentén tovább finomult a szakterületi feladatrendszer. Az együttműködés, képzés és gyakorlás, valamint a kibervédelmi gyakorlatok képezik a hangsúlyt a technikai kérdések, módszerek és eljárások mellett.

A másik jellegzetes gondolat a katonai műveletek támogatása (a kibertér területén is „műveletivé" kell alakítani a gondolkodást), ugyanakkor a nemzetközi normák betartása továbbra is kötelező. A katonai műveleteknél a védelemtől eltérő jelleg – a „kibertér hatás" került elő, benne a nemzetek önkéntes támogatási mechanizmusával.

A megnyitó beszédeket követően két, magas szintű kerekasztal-beszélgetésre került sor, melyek során a NATO, illetve a tagállamok meghívott vezető beosztású tisztségviselői cseréltek eszmét a *kibertérből érkező fenyegetésekről és kihívásokról*, valamint a *Kibervédelmi Kötelezettségvállalásról*.

Fenyegetések

A kibervédelmi képességek fejlesztése alapvetően nemzeti felelősség és ebből következően a NATO, mint szövetség *csak akkor fog hatékony kibervédelemmel rendelkezni, ha valamennyi tagállam biztosítja saját rendszereinek védelmét*. A kibertér fenyegetései modern életünk részévé vált, de a más fenyegetésektől eltérően az állami és nem állami szereplők megkülönböztetése és a kémkedés elleni védelem kiemelt feladattá vált.

Francia vélemény szerint gyorsabb – a civil és a kormányzati rendszereknél egyaránt fontos – védelmi megoldásokra van szükség, gyorsítani kell a döntéshozatal rendszerét, a technikai kérdések mellett a diplomácia támogatás és az etika kérdései is előtérbe kerültek. Fontos üzenet, hogy a nemzeteknek meg kell tanulni együttműködni, a használható megoldásokat azonnal adoptálni kell, illetve a kormányzati és a társadalom elemei között azonnali (real time) együttműködésre van szükség. A szakértői bázis kialakítása és fenntartása érdekében új szervezeti és működési modelleket kell kialakítani.

---

[3] Ez a kifejezés jelenik meg – ilyen formában először – két hónappal később a NATO Brüsszeli Csúcsértekezleten. Brussels Summit Declaration 2018. 07. 09. https://www.nato.int/cps/en/natohq/official_texts_156624.htm, p. 20. (Letöltés ideje: 2018. 09. 24.)

A nemzetközi együttműködés kiemelt jelentőségű, ahol *első lépés a megbízhatóság kérdésének rendezése (trusted partnership)*, (ugyanez bilaterális együttműködés esetében is), illetve *meg kell oldani a kompatibilitás kérdéseit technikai és eljárási, szabályozási szinteken egyaránt*.

Diplomácia területen ki kell emelni, hogy „a diplomatáknak nem csak akkor kell dolgozni, amikor már baj van". A bizonyítékok, technikai jellemzők (attributum) azonosítása még nem kiforrott, így a diplomácia eszkalációt megakadályozó szerepe megerősödik. Az export korlátozás kérdését is fejleszteni lehetne (hogyan lehet követni, megakadályozni adott termékek mozgását), vizsgálni kell az aktív védelem lehetőségeit (hogyan lehetne védelmet biztosítani nem csak monitoring megoldásokkal, hanem műveletekkel, hogyan lehet ezt a kérdést szabványosítani. A szoftver beszállítók felelősségét is újra kell gondolni: *amennyiben a szoftverhiba miatti sérülékenység valakinek kárt okoz, hogyan lehet a biztonságot garantálni, illetve a kárt téríttetni*.

A stratégiai kommunikáció (STRATCOM) szerepe a kibertér (vagy kibervédelem) esetében is többfunkciós, a tájékoztatás, média és az elrettentés feladatait szolgálja.

EU szinten a civil, katonai hálózatok kapcsolódása – és az ezzel kapcsolatos fenyegetések növekedése – aláhúzza a civil és kormányzati szektor közötti együttműködés fontosságát. Fontos kérdés, hogy az államok függetlensége érdekében (souvereignity) mit kell tenni a kibertérben nemzeti és nemzetközi szinten, hogyan valósítható meg ezeken a szinteken a biztonsági kérdések irányítása (governance).

A függőségek (dependence) azonosítása kulcskérdés és azt is *jobban meg kell érteni, hogy az egyes szereplők miért viselkednek eltérően* (pl. pénzügyi szektor, szoftvercégek, kritikus infrastruktúra üzemeltetők). Normákat kell kialakítani az alap (core) infrastruktúra támadhatóságának csökkentése érdekében, ami nem csak jogi kérdésnek tekintendő. A különböző területeken a szabályozás fejlődésével a szereplők pontosításokat tehetnek, új normákat alakíthatnak ki.

Megindult a szoftver-sérülékenységek feltárásával kapcsolatos (software vulnerability disclosure) kérdések komolyabb vizsgálata, eljárások kidolgozása, mert egy kis hardver- vagy szoftverhiba alacsony szakmai tudás esetén is könnyen kihasználható. Kérdés, hogyan lehet biztonságos eljárásokat kidolgozni, a fejlesztőket, gyártókat javításra kötelezni, a termékek garanciáinak kérdését rendezni, illetve piaci szereplők számára egyenlő feltételeket biztosítani.

A NATO szerepe a kibervédelem területén abban ragadható meg, hogy *fórumot biztosít a tagállamok közötti együttműködés számára*. Rose Gottemoeller NATO főtitkár-helyettes megfogalmazásával élve – a kibervédelem csapatjáték (*„cyber defence is a team sport"*), a hatékony kibervédelem együttműködés nélkül elképzelhetetlen. Az együttműködés területén a kormányok, nemzetközi szervezetek mellett *nem szabad megfeledkezni az ipari szereplőkről, oktatási intézményekről* sem.

A kollektív védelem kérdésénél a kollektív elrettentést is említeni kell, mely területen normatív szabályokat, eljárásokat kell kidolgozni. Növelni kell a rendszerek ellenállóképességét (resilience), – gyorsabb reagálás, nagyobb hatékonyság szükséges –, fejleszteni kell a kibertér higiéniáját (cyber hygenie).

A NATO műveletek sikere érdekében *ki kell emelni a vezetés fontosságát, amit a kibertér-műveletek esetében is értelmezni, fejleszteni kell.*

A fenyegetésekre vonatkozó blokk összefoglalása, hogy *a kibertér műveleti területként való alkalmazásának kinyilvánítása*[4] *(domain) egymástól való tanulást is jelent* négy fő területen (technológia, ember, eljárás és szervezet).

Erősíteni kell a hálózatok ellenállóképességét, növelni kell a hálózatok biztonságát és a minőséget, figyelni kell a katonai műveletek összes spektrumú támogatására (NATO szinten: a Szövetségnek jobban műveleti jellegűnek kell lennie). Ennek érdekében azonosítani kell, hogy stratégiai, politikai szinten melyek a feladatok annak érdekében, hogy az erőforrások felhasználása helyesen történjen.

Kibervédelmi Kötelezettségvállalás (Pledge)

Francia vélemény szerint a kibertér biztonsága „törékeny dolog". Vészhelyzetben azonnali beavatkozásra van szükség, fontos a szereplők között az információmegosztás, illetve a kockázatalapú gondolkodás. Mindenki felelős a saját hálózat védelméért nemzeti szinten, ugyanez a NATO feladata is, valamint az EU NIS irányelv is hasonlóan működik (hálózatok védelme és információmegosztás).

A NATO közvetítő szerepet játszik (hub), közös gyakorlatok rendezésén keresztül nyújt szakmai segítséget, illetve a Pledge-n keresztül támogat.

Nemzeti, szervezeti szinten az együttműködés segíthet, mert lehet tanulni egymástól, a működő modellek más helyen is alkalmazhatók. Az e területen tapasztalható kibertér műveleti parancsnokságok csak egy megoldásnak tekinthetők („akár következhet kiber ezred is"), a hangsúly a szervezeti hatékonyságon van.

Az észt vélemény hasonló fogalmazású volt, mely szerint „a saját házat mindenkinek rendben kell tartani". A Locked Shields nemzetközi kibervédelmi gyakorlat segíti a gyakorlati szemlélet terjedését (a katonai és kritikus infrastruktúra elemek közös gyakoroltatása történt), ahol előkerülnek az azonosított helyzetkép kérdései és az azonosításhoz szükséges jellemzők fontossága. A kibervédelmi gyakorlatok valóság közeli forgatókönyvei segítenek annak bemutatásában, hogy a kibertér műveleteknek milyen hatásai lehetnek, illetve azokra milyen válaszokat kell adni.

Fontos kérdés azonban annak megértése, hogy a gyakorlat csak teszt. A valós életben a vezetésnek, a technikai állománynak folyamatosan aktívnak kell lennie, a kibertér fenyegetési információk gyűjtése, *az aszimmetrikus kihívások kezelése napi feladat és nem csak eseti jellegű tevékenység.*

A Pledge – mint közös keretrendszer – segít a gondolkodásban, illetve a politikai támogatáshoz ad segítséget (a politikai szintnek tudatában kell lennie a helyzettel és a szükséges teendőkkel).

Cseh tapasztalat, hogy a Pledge gyorsította a nemzeti folyamatokat, így 2017-ben önálló Nemzeti Kibervédelmi Hatóság alakult, ami a Védelmi Minisztériumnál segítette a feladatok prioritásainak felállítását, a felelősök és feladatok meghatározását. *A gyakorlatok jó lehetőségeket biztosítanak annak elismerésére, hogy a kibertéri hatásokra milyen politikai válaszokat kell adni.* A cseheknél is jelentkezik a nemzetközi szinten is azonosítható szakképzett munkaerőhiány, a pótlást az egyetemeken történő toborzással próbálják megoldani.

---

[4] NATO Warsaw Summit Communiqué 2016. 07. 08-09., https://www.nato.int/cps/ic/natohq/official_texts_133169.htm, p. 70. (Letöltés ideje: 2018. 09. 24.)

A délelőtti kerekasztal-beszélgetések során Antonio Missiroli, a NATO-főtitkár új típusú biztonsági kihívásokért felelős helyettese röviden beszámolt a Szövetség keretében elfogadott Kibervédelmi Kötelezettségvállalás végrehajtásának helyzetéről is.

A kötelezettségvállalás alapvetően a politikai eszköztárba tartozik és nem részletes, technikai kézikönyv. A kötelezettségvállalás jelentősége abban áll, hogy támogatja a kibervédelem területén kifejtett nemzeti erőfeszítéseket azáltal, hogy egyrészt segít fenntartani a téma iránti politikai figyelmet, másrészt általános iránymutatást nyújt a tagállamok vonatkozó képességfejlesztési erőfeszítéseihez.

Részletek említése nélkül súlyponti kérdésnek kell tekinteni az *információmegosztást (szegregáció felszámolása)*, a *releváns ipari szereplők bevonását (beszerzés, kutatás-fejlesztés)* és a *biztonságtudatosság részeként a kommunikáció, tömegtájékoztatás fejlesztését*.

Elmondható, hogy *a nemzetek kiemelt feladata az azonosítással (attribution) kapcsolatos kérdések helyes kezelése* a hatékony válaszlépések érdekében, a hálózatok ellenállóbbá tétele, az elrettentéshez szükséges kibertér-képességek azonosítása.

Összefoglalásként elmondható, hogy a Kibervédelmi Kötelezettségvállalás egy olyan stratégiai szintű hét részből álló szempontrendszer, ami szempontokat adhat a nemzetek képességfejlesztéséhez.[5] A napi élet kihívásai, vagy új szolgáltatások, esetleg fenyegetések megjelenése esetén a reagáláshoz szükséges megoldás a szempontrendszerbe illeszthető, vizsgálhatók az együttműködési kérdések, illetve egységesebbé válhat a nemzetek közötti konzultáció. A gyakorlatilag nemzeti szintű kérdések megfogalmazása jelzi, hogy nem csak kifejezett katonai képességekről van szó, így a nemzeti szintű oktatási, együttműködési gyakoroltatási kérdések, a létfontosságú infrastruktúra-védelem mellett meg kell oldani a stratégiai szintű szabályozási, nemzetközi együttműködési kérdéseket, meg kell felelni a nemzetközi jogi normáknak is.

A dán stratégia további érdekessége, hogy a nemzetközi irodalomban még nem gyakori megoldásként elkülöníti az elektronikus információvédelem és a kibervédelem szakterületét. Az egyre népszerűbb kibervédelmi szemlélet ezt a „szakosodást" gyakran figyelmen kívül hagyja, melynek az is indoka, hogy napjainkban a „kiber" előtaggal jelzett témákkal lehet sikeresen érvelni, ami feladatokban, együttműködési kérdéseken torzulásokhoz vezethet.[6]

A kerekasztal-beszélgetéseket követően délután a konferencia szakértői szintű workshopokkal ért véget, amelyek keretében a tagállami szakértők az erőforrás-allokáció, az információmegosztás, a kiképzés, oktatás és gyakorlatok, valamint a kiberműveleti központok felállítása kapcsán oszthatták meg egymással tapasztalataikat.

---

5 NATO Cyber Pledge, (I-VII. p.) https://www.nato.int/cps/en/natohq/official_texts_133177.htm, 5. p. (Letöltés ideje: 2018. 09. 24.)

6 Danish Cyber and Information Security Strategy, 2018, https://uk.fm.dk/publications/2018/danish-cyber-and-information-security-strategy, p. 7. (Letöltés ideje: 2018. 09. 24.)

Erőforrások

Az erőforrások címet viselő workshop a brit, illetve a holland kiberbiztonsági politika aktualitásaiba adott betekintést.

Az Egyesült Királyság első Nemzeti Kiberbiztonsági Stratégiáját (National Cyber Security Strategy) 2011-ben fogadták el. Ezt a 2011-es dokumentumot 2016-ban váltotta fel az ország jelenleg is érvényben lévő Nemzeti Kiberbiztonsági Stratégiája, amely a 2021-ig tartó időszak feladatait foglalja össze. A dokumentumban megjelölt legfőbb célkitűzés, hogy *az Egyesült Királyság olyan ország legyen, ahol a kiberbiztonság magas szintje támogatja a gazdaság működését*.

A stratégia három fő pilléren (védelem, elrettentés és fejlesztés) nyugszik. Az első, védelmi pillér azt tűzi célul, hogy *az ország rendelkezzen azokkal az eszközökkel, amelyek ahhoz szükségesek, hogy megvédje magát a kibertérből érkező fenyegetésekkel szemben*, hogy hatékonyan reagáljon a bekövetkező incidensekre, valamint hogy biztosítsa hálózatai, adatai és rendszerei védelmét.

A második, elrettentési pillér arra vonatkozik, hogy *az Egyesült Királyság olyan állam legyen, amelyet nem éri meg a kibertérből fenyegetni*. Ennek érdekében az ország ellen irányuló ellenséges akciókat felderítik, a támadókat pedig felelősségre vonják. Ehhez kapcsolódóan napjainkban sokat vitatott kérdés az attribúció, tehát a támadók nyilvánosság előtti megnevezésének gyakorlata. Az ország azt az elvet követi, hogy attribúcióra *minden olyan esetben sor kerül, amikor az a nemzet érdekeiket szolgálja*.

Végezetül a harmadik, fejlesztési pillér azt mondja ki, hogy *az Egyesült Királyság innovatív és növekvő kiberbiztonsági iparral kell hogy rendelkezzen, amely mögött világszínvonalú kutatási és fejlesztési háttér áll.*[7]

A fenti célok elérése érdekében a brit kormányzat ún. intervencionista stratégiát alkalmaz, amelynek keretében – többek között – felállították a Nemzeti Kiberbiztonsági Ügynökséget (National Cyber Security Agency, NCSA), valamint jelentős forrásokat különítettek el a védelmi és a támadó kiberképességek fejlesztésére. Az NCSA feladata, hogy támogassa a közszféra, az ipar, valamint a kis- és középvállalkozások kiberbiztonsági erőfeszítéseit. Ennek keretében az ügynökség gyakorlati útmutatókat dolgoz ki és tesz közzé, tanácsadást nyújt, képzéseket szervez, valamint segíti a kiberbiztonsági incidensek kezelését és az azokra való válaszadást.

Hollandia aktuális Nemzeti Kiberbiztonsági Stratégiáját (National Cyber Security Agenda – A cyber secure Netherlands) 2018. április 21-én tették közzé. A stratégia abból indul ki, hogy Hollandia a digitális értelemben legfejlettebb országok közé tartozik, ami számos gazdasági és társadalmi előnnyel jár. Emellett nem szabad megfeledkezni arról, hogy a digitalizáció adta előnyökkel az ország csak abban az esetben tud élni, ha kellő gondot fordít a digitális szféra biztonságára. A kibertérből érkező fenyegetések száma és komplexitása jó ideje növekszik és a belátható jövőben is ennek a trendnek a folytatódása várható. Ezt felismerve döntött úgy a holland kormányzat, hogy további lépéseket tesz az ország kiberbiztonságának

[7] National Cyber Security Strategy 2016-2021, Implementation Plan (p. 32-60) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, pp. 5-7. (Letöltés ideje: 2018. 09. 24.)

megerősítése érdekében, a szükséges intézkedéseket pedig a kiberbiztonsági stratégiában foglalták össze.

A stratégia az alábbi hét alapelven nyugszik:

1) a kiberbiztonság szerves része a nemzetbiztonságnak;
2) a köz- és a magánszféra együttműködése elengedhetetlen a digitális szféra biztonságának garantálásához;
3) a kormányzat a közszféra kiberbiztonságáért felel;
4) döntő fontosságú az információmegosztás és a kutatói háttér fejlesztése;
5) a kiberbiztonsági szempontokat be kell építeni valamennyi szervezet mindennapi működésébe;
6) a digitális világban a fizikai határok nem értelmezhetők;
7) a szabadság és a biztonság közötti feszültség természetes velejárója a digitális forradalomnak.

A Stratégia által elérni kívánt cél, hogy Hollandia képes legyen biztonságos módon kihasználni a digitalizációból fakadó gazdasági és társadalmi előnyöket, illetve megvédeni a nemzetbiztonságot a digitális szférában is. A célok elérése érdekében Hollandiában hét feltételnek kell teljesülnie:

1) a kibertérből érkező fenyegetések felismeréséhez és az azokra való határozott válaszadáshoz szükséges digitális képességek rendelkezésre állása;
2) hozzájárulás a nemzetközi békéhez és biztonsághoz a digitális világban;
3) biztonsági szempontból a világ élvonalába tartozó hardverek és szoftverek használatának ösztönzése;
4) a kiberfenyegetésekkel szemben ellenálló digitális eljárások és robosztus infrastruktúra fenntartása;
5) a kiberbűnözést ellehetetlenítő akadályok felállítása;
6) a kiberbiztonsággal kapcsolatos ismeretek bővítése és világszínvonalú kutatói háttér megteremtése;
7) szoros együttműködés az állami és a magánszféra között.[8]

Oktatás, képzés és gyakorlatok

Az oktatásért és képzésért felelős szekció moderálását NATO és Kanada vállalta magára, bevezetésként kiemelve, hogy a képzés szerves részeként kell kezelni a gyakorlatok rendszerét, az ezzel kapcsolatos eljárások fejlesztése elsődleges prioritásúnak tekintendő.

A NATO felülvizsgálja a korábban kialakított oktatási rendszert, az elektronikus információvédelem[9] alapjain kívánja megteremteni a kor követelményeinek megfelelő, kibertér képességek támogatását célzó struktúráját.

---

[8] National Cyber Security Agenda - A cyber secure Netherlands, 2018, https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html, p. 7. (Letöltés ideje: 2018. 09. 24.)

A jelenleg több helyszínen folyó képzések racionalizálása megkezdődött, a párhuzamos tanfolyamok azonosítása folyamatban van. Ez érinteni fogja a képzésért és oktatásért felelős szervezetek felépítését és szervezeti elhelyezkedését is.

Észtország a Locked Shield nemzetközi kibervédelmi gyakorlat tapasztalatait integrálja az oktatási rendszerébe, szoros együttműködésben a NATO CCD COE szakembereivel. Hiányosságként azonosítható az a szakértői réteg, akik képesek a technikai csapat és a politikai, döntéshozatali szintek közötti kommunikáció megvalósítására. A közös, mindenki számára érthető nyelvezet magas prioritást kell hogy kapjon, ellenkező esetben nem garantálható konzekvens döntés.

A kommunikációs „hidat" képező személyek képzésére külön figyelmet kell fordítani, a tematika kialakítását mihamarabb meg kell kezdeni. Külön nehézség ebben az esetben, hogy a kiválasztott személyeknek rendelkezni kell a terület teljes átfogó ismeretével, döntéshozatali és technikai jellegű háttértudással, alapvető jogi ismeretekkel és kommunikációs képességekkel.

A döntéshozókat „döntésekre kell kényszeríteni" a gyakorlatok folyamán, hiszen a valós életben is ez lesz majd a feladatuk. Fel kell készülni a döntéshozók olyan kérdéseire, hogy „Mit tehetek, és hogyan kommunikálom majd?"– ezekre konkrét válaszokat kell adni. Ha a vezető nem elkötelezett, a feladat megoldása nem lehet sikeres. A bizalmat erősíteni kell a nemzetközi környezetben és erősíteni kell az információmegosztást is.

Az észt, valamint spanyol tapasztalatok azt mutatják, hogy közös katonai jellegű gyakorlatok esetén a műveletekkel kapcsolatos általános eljárásrendek már mindenki számára ismertek, azok működőképesek, azonban a kibertér-terület még nincs megfelelően szabályozva és integrálva. A közös együttműködés fontosságát nem lehet eléggé hangsúlyozni, hiszen az egymástól való tanulás nagymértékben felgyorsítja a kibertérben történő folyamatokra adott válaszok sebességét.

Összefoglalásként elmondható, hogy több nemzet egybehangzó tapasztalatai azt mutatják, hogy nem külön kibervédelmi gyakorlatokat kell szervezni, hanem komplex módon a kiberteret szerepeltetni kell a gyakorlatokban, valóságközelivé kell tenni minden domain számára.

Kiemelt követelmény, hogy meg kell érteni magát a kiberteret, mint speciális környezetet, figyelemmel kell kísérni annak változásait. A műveletek tervezésének szerves részét kell hogy képezze a kibertéri feladatrendszer, erőforrást kell biztosítani arra, hogy egy-egy feladat végrehajtása során a megfelelő modulok kerüljenek integrálásra (mission specific training).

A több vonalon megjelenő toborzás, szakértői szintű munkavállalók megtartása az egyik legfontosabb kérdésnek mutatkozott ugyanúgy, mint Knapp Gábor és Király Ágnes cikkében[10] bemutatott útkeresések az 2017-es budapesti EUCOM szimpóziumon elhangzottak szerint.

---

[9] Korábban INFOSEC – (electronic) information security, a kétezres évek első évtizedének közepétől Information Assurrance (IA).

[10] KIRÁLY Ágnes – KNAP Gábor: A III. Nemzetközi Kiber(tér) Szimpózium – 2017. Budapest; Szakmai Szemle, HU ISSN 1785-1181, 2017/2. p. 138, 140 és 142.

Műveleti kérdések

Az olasz Összhaderőnemi Műveleti Kibertér Parancsnokság (Joint Operations Cyber Command – JOCC) feladata a katonai rendszerek védelme otthon, misszióban vagy külföldi állomáshelyeken, illetve felkérésre nemzeti segítség nyújtása (tartalékok rendelkezésre bocsátása, kritikus infrastruktúra-védelem vagy katasztrófa-felszámolás).

A JOCC a vezérkar főnök alárendeltségébe tartozik, felügyeli a katonai eseménykezelő koordinációs központot (milCERT) és együttműködik a hazai hatáskörű hírszerzéssel. A koordinációs központhoz van bekötve mindhárom haderőnem szakmai szervezete (szárazföldi, légi és haditengerészeti elemek) és a katonai csendőrség.

A JOCC hatáskörébe nem tartozik bele az üzemeltetés, védelmi kérdésekben tanácsot adnak, ami nehézkes megoldásokat eredményez (a jövőben ezen a területen valamilyen változást kell kidolgozni).

Fejlődési vonalként a kibervédelemről való áttérés a kibertér-műveletekre lépésként azonosítható.

Kulcskérdés az *infrastruktúra védelem és fejlesztés* („nem elégséges tízévente hardvert cserélni"), a *szervezetfejlesztés*, a *laboratórium és virtuális gyakorlótér* (cyber range), valamint a *személyi utánpótlás* biztosítása („akár az utcáról is lehessen szakembert felvenni").

A beszerzéseknél új, korszerű megoldásokat kell kialakítani, mert a nemzeti arány nem elégséges (a multinacionális cégek túlsúlyban vannak).

A kritikus infrastruktúra-védelem esetében különböző eseteket kell figyelembe venni (békeállapot vagy egyéb, beleértve a háborút is), illetve más a bűnüldözés és a fegyveres erők feladatrendszere, így védelmi területen a JOCC feladata kizárólag a katonai rendszerek védelme.

A német szakmai ismertetés lényegi mondanivalója a hálózatok centralizációja és az ezzel kapcsolatos gondolkodás volt. Korábban több százas nagyságrendű kiszervezett szolgáltatásokra támaszkodtak, 2017-től ez a rendszer teljesen átalakult centralizált katonai tulajdonú és üzemeltetésű rendszerré („military owned"). A tudatos centralizálás („no regional separation") célja az erőforrás-takarékosság és a hatékonyabb működés.

2016-ban alakult ki a Védelmi Minisztérium „Cyber IT Directorate (CIT)" két részterületre bontva: Stratégiai és Tervező Főosztály: Berlin, Üzemeltetés és Információvédelmi Főosztály: Bonn és a „Cyber and Information Domain Service HQ (CIDS)" kettős szerepkörrel.

A CIDS fő elemei:

- SIGINT;
- katonai hírszerzés (nem részletezett feladatokkal);
- számítógép-hálózati műveletek (Computer Network Operations – CNO) és
- elektronikai hadviselés (EW).

A súlyosnak tekintett szakképzett munkaerőhiány kérdésre tartalékos keretben gondolkodnak („Cyber Reserve Personal Pool"), amelyben 18-45 év között, kategóriákra osztva dolgoztak ki bonyolult rendszert:

- katonai szakképzettségű, de pályát elhagyók (katonai beosztásra);
- katonai képzettség nélküliek (katonai-civil beosztásra);

– kibertér-közösségbe tartozó személyek („cyber community") – nem szükséges státuszba venni;
– egyedi kategória gazdaság, tudomány, ipar területéről – dedikált feladat esetén (katonai-civil beosztásra szakértőnek, tanácsadónak).

Új kezdeményezés a *dedikált szervezeti elem felállítása a jövőkutatás érdekében* („Cyber Innovation Hub"). Fő feladatai:
– a digitalizáció kérdéseinek vizsgálata (egyre nagyobb számú elektronikus eszköz kerül a rendszerbe, melyeket szükségszerűen integrálni kell, melyet egységes elgondolás alapján lehet végrehajtani);
– a jövőbeli technológiák („future technologies") keresése, a 2030-2035 körüli információs környezet jellemzőinek kutatása;
– az ellenállóképesség (resilience) kérdéseinek vizsgálata;
– a kibertér „műveletesítése" („operationalisation of cyber") feladat értelmezése, megoldások keresése (beleértve a parancsnokok, vezetők képzését, a „hogyan lehet vezetni" abban az esetben, ha nincs, vagy csak csökkentett IT szolgáltatások állnak rendelkezésre.

A szervezetbe tehetséges katonákat, tartalékosokat és közalkalmazottakat toboroznak.[11]

A francia ismertetés (CYBERCOM) bemutatta, hogy a 2010-es alapítás után szervezeti átalakítást végeztek 2017-ben. A „művelet" (mint kibertéri tevékenység) egyaránt jelent: *detektálást, missziós támogatást* és *reagálási képességet* (védelem, kibertér támadásra történő reagálás, propaganda és dezinformáció detektálás).

A szervezetfejlesztésnél kifejezett anomália, hogy *gyors fejlesztést kellene végrehajtani, ugyanakkor a szakértők kiképzése, toborzása egyre nehezebbé válik.*

A Parancsnokság a vezérkar főnök közvetlen alárendeltségében van, együttműködik a hadművelettel, ellátja a minisztert szakmai tanácsokkal.

Szakmai érdekesség, hogy a kormányzati eseménykezelő szervezet (GovCERT) és a katonai eseménykezelő szervezet (milCERT) közös szervezetbe integrált, ami a francia tapasztalat szerint hatásfokot növelő tényező.

A nemzeti ismertetések után egy központi kérdés köré épült csoportos beszélgetés bontakozott ki: *hogyan lehet mérni a kibertéri műveleti képességek hadműveleti készültségét,* mikor válik „hadrafoghatóvá" a kibertér-erő?

Az összegzett válasz lényege, hogy csak „magas szinten" célszerű gondolkodni, részletes mérési paraméterek kidolgozására, mérésre és elemzésre, kiértékelésre egyszerűen nincs még jó megoldás (nincs értelme, hogy „ugyanakkora állomány mérjen és ellenőrizzen, mint a végrehajtók"). Emiatt a NATO Pledge-t sem célszerű részletesebb paraméterekkel „hígítani".

Német tapasztalat, hogy *a kulcsfontosságú paramétereket kell azonosítani és követni*. A centralizált infrastruktúra esetén csak a szolgáltatási szerződési modellel lehet jól dolgozni (SLA) – azaz pontosan ki kell dolgozni, hogy melyek a nyújtott IT szolgáltatások, azokra kik jogosultak, melyek a szolgáltatásigénylés, biztosítás pontos szabályai, melyek a szolgáltatók feladatai és melyek a szolgáltatásmódosítás

[11] Cyber and Information Domain, http://cir.bundeswehr.de/portal/a/cir/start/presse/pressematerial/Flyer Organisationsbereich Cyber- und Informationsraum, p. 1. (Letöltés ideje: 2018. 09. 24.)

szabályai (szolgáltatói oldalról vagy igénylő oldaláról egyaránt). Ezt a modellt a kibertér-kérdések esetén is lehet követni.

Összefoglalás

A konferencia kapcsán összefoglalásként elmondható, hogy a NATO Kibervédelmi Kötelezettségvállalás mögötti feladatrendszer a kialakításra vonatkozó 2016-os Varsói Csúcstalálkozón hozott döntés óta folyamatos fejlődésen ment keresztül.

Kialakult egy stratégiai szintű vizsgálati szempontrendszer, melynek során előkerült a mérhetőség, összehasonlíthatóság kérdése. Az eltérő értelmezések közelítése érdekében bilaterális jellegű konzultáció formájában szövetségi feladat született az éves ismétlődésű önellenőrzések során felhalmozódott tapasztalatok hasznosítása érdekében. A kiegészítő támogatásként értékelhető konferencia lehetőséget teremtett a konzultációra és a közös gondolkodásra.

Tartalmi szempontból igazolható, hogy *a korábban gyakran csak technikai feladatokban elképzelt kibervédelem ennél lényegesen bonyolultabb feladatokat, folyamatokat tartalmaz*.

A kibervédelmi gyakorlatok tapasztalatai erősítik, hogy a szükséges együttműködések, információmegosztás nélkül a feladatok megoldása kétséges.

A gyakorlati élet, a katonai feladatok sokszínűsége mutatja, hogy technikai szinten is összetett gondolkodásra van szükség. Az analóg rádiózástól kezdve a kritikus infrastruktúra elemeknél alkalmazott 15-20 éves ipari vezérlőrendszerek szoftverein keresztül már a gépi tanulás, a mesterséges intelligencia alkalmazása (sajnálatos módon nem csak a védelmi mechanizmusokban), a várható kvantum-számítástechnika kérdései is bővítik a kihívások körét.

A kibertér, mint műveleti terület megfogalmazás új feladatokat szab a katonai műveletek teljes életciklusában. Ez rámutat arra az új szempontra is, hogy *a kibertérben szükséges védelmi feladatokat nem elégséges oktatóközpontokban, laborokban „lejátszani", hanem a valós, problémákkal teli katonai műveletek során is meg kell tudni oldani*.

Ugyanígy látható az is, hogy *az egyre összetettebb feladatokat nem lehet az informatikai szakterületre terhelni*, mert a komplex kibervédelmi gondolkodás összetettebb technikai megoldásokat, szakmai együttműködést – akár kísérletezést is – igényel, mely feladatokat nem lehet az informatikai üzemeltető állomány „nyakába varrni".

Az összetettség új szakmai kapcsolatokat, döntésekhez szükséges vezetéstámogatási lépéseket kíván, melyeket nem lehet a hagyományos, 15-20 év alatt kialakult keretek rendjében kezelni.

A műveleti terület kérdése súlyponteltolódást kell, hogy jelentsen a hagyományos védelmi típusú gondolkodáshoz képest. A katonai művelet milyen kibertérben történő műveletekkel támogatható? *A kinetikus világban megszokott kérdéseket, mint az ellenfél lehetőségeinek korlátozása, az erőfölény átbillentése a kibertérben is értelmezni kell*, melynek során az információgyűjtés, egymásra épülő lépések hatásainak tervezése és végrehajtása megfogható technikai, szervezeti feladatokat kell hogy jelentsen.

A francia példa mutatja, hogy érdemes a különböző alárendeltségben lévő szervezeti elemekkel kísérletezni. A közösen kialakított szervezetek, vagy a szervezetek közötti időszakos keresztbefoglalkoztatás vagy egyéb delegációs

megoldások *jól működhetnek, de csak kialakult szakmai kultúra és rögzített eljárások esetén.*

A fenti kérdések áttekintése jól mutatja, hogy hazánkban a honvédelmi szakfeladatoknál megjelent és erőteljesen részletesebbé válik a kibertér-műveleti feladatrendszer, melynek megértése, szabályozása, katonai feladatokba történő integrálása, illetve az ehhez szükséges támogató pillérek kialakítása olyan nem megkerülhető kérdés, ami hosszú éveken keresztül feladatokat jelent majd vezetői és végrehajtói szinten egyaránt.

Felhasznált irodalom:

- Brussels Summit Declaration 2018. 07. 09. https://www.nato.int/cps/en/natohq/official_texts_156624.htm, p. 20. (Letöltés ideje: 2018. 09. 24.)
- Cyber and Information Domain, http://cir.bundeswehr.de/portal/a/cir/start/presse/pressematerial/Flyer Organisationsbereich Cyber- und Informationsraum, p. 1. (Letöltés ideje: 2018. 09. 24.)
- Danish Cyber and Information Security Strategy, 2018, https://uk.fm.dk/publications/2018/danish-cyber-and-information-security-strategy, p. 7. (Letöltés ideje: 2018. 09. 24.)
- KIRÁLY Ágnes – KNAP Gábor: A III. Nemzetközi Kiber(tér) Szimpózium – 2017. Budapest; Szakmai Szemle, HU ISSN 1785-1181, 2017/2. p. 138, 140 és 142.
- More than 1000 cyber experts from 30 nations took part in Locked Shileds, https://ccdcoe.org/more-1000-cyber-experts-30-nations-took-part-locked-shields.html, (Letöltés ideje: 2018. 09. 24.)
- NATO Warsaw Summit Communiqué 2016. 07. 08-09., https://www.nato.int/cps/ic/natohq/official_texts_133169.htm, p. 70. (Letöltés ideje: 2018. 09. 24.)
- NATO Cyber Pledge, (I-VII. p.) https://www.nato.int/cps/en/natohq/official_texts_133177.htm, 5. p. (Letöltés ideje: 2018. 09. 24.)
- National Cyber Security Strategy 2016-2021, Implementation Plan (p. 32-60) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, pp. 5-7. (Letöltés ideje: 2018. 09. 24.)
- National Cyber Security Agenda – A cyber secure Netherlands, 2018, https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html, p. 7. (Letöltés ideje: 2018. 09. 24.)

E SZÁMUNK TARTALMA

DR. HABIL. RESPERGER ISTVÁN

AZ ISZLÁM ÁLLAM TERRORSZERVEZET LAKOTT TERÜLETEKEN FOLYTATOTT HARCAINAK KATONAI TAPASZTALATAI

A tanulmány célja az Iszlám Állam lakott településen és a beépített területen folytatott tevékenységének elemzése. Több esettanulmány (Moszul, Daraa, moszuli gátrendszer), továbbá a Ninive tartományban folytatott katonai és rendőri tevékenység kerül hadtudományi szempontból bemutatásra. Az elemzés a lakott területeken folytatott küzdelem forgatókönyvét mutatja be a tanulságok levonásával.

Kulcsszavak: hadtudomány, Iszlám Állam, lakott területen folytatott harc, mesterlövészek, tervek, módszerek, eljárások.

DR. LÁSZLÓ VIKTÓRIA

A BIZTONSÁGOT VESZÉLYEZTETŐ TÉNYEZŐK, AZOK HATÁSAI ÉS KÖVETKEZMÉNYEI NAPJAINKBAN

A megváltozott biztonsági környezet hatásaival, különböző megnyilvánulási formáival nap mint nap - közvetetten mindenképpen - szembesülünk, hiszen a különböző infokommunikációs csatornákon keresztül folyamatosan elárasztanak bennünket a terrortámadásokról, a migrációról, a természeti katasztrófákról stb. szóló hírek, információk.

Dolgozatomban a tudományos irodalom forrásaira támaszkodva - a teljesség igénye nélkül - áttekintem a biztonság fogalmának bővülését, a XXI. század globális biztonsági kihívásait, kockázatait, fenyegetéseit. Kísérletet teszek a biztonságot veszélyeztető tényezők főbb jellegzetességeinek, a legfontosabb tendenciáknak és folyamatoknak a bemutatására, külön vizsgálva a hazai vonatkozásokat is.

Napjainkban a biztonságra globális szinten negatívan ható tényezők a világ minden pontján, így Magyarországon is kisebb-nagyobb mértékben, közvetve vagy közvetlenül érintik az emberek mindennapjait, valós veszélyt jelentenek, ezért ezekkel a problémákkal foglalkozni kell, azok megoldására válaszokat kell keresni és találni.

Kulcsszavak: biztonság, biztonsági környezet, biztonsági kihívások, kockázatok, fenyegetések, biztonságot veszélyeztető tényezők

CONTENTS

ISTVÁN RESPERGER DR. HABIL.

LESSONS LEARNED OF FIGHTS CARRIED OUT BY THE ISLAMIC STATE TERRORIST ORGANISATION IN INHABITED AREAS

The purpose of the study is to analyze the activity of the Islamic State in inhabited settlements and areas. Several case studies (Mosul, Daraa, Mosul dam system) and military and police activities in the Nineveh province are presented from a point of view of military science. The analysis illustrates the scenario of the struggle in populated areas and also the lessons learned.

Keywords: Military Science, Islamic State, fighting in an urbain terrain area, snipers, plans, methods, procedures

VIKTÓRIA LÁSZLÓ DR.

SECURITY-THREATENING FACTORS, THEIR IMPACTS AND CONSEQUENCES IN OUR DAYS

We are confronted with the effects of different security environments and with different forms of manifestation day by day – indirectly definitely - as news about terrorist attacks, migration, natural disasters, etc. are constantly flooding through various info communication channels.

In my study, I lean on the sources of scientific literature, without the necessity of completeness, to consider the expansion of the concept of security, Global Security Challenges, Risks, and Threats of the Century. An attempt is made to present the main features, the most important trends and processes of security-threatening factors, by examining the domestic aspects separately.

Nowadays, different types of factors have a negative effect on global security all around the world, so in Hungary. These factors affect people's lives more or less directly or indirectly and they pose a real threat. Therefore, these problems need to be addressed and answers need to be found.

Keywords: security, security environment, security challenges, risks, threats, security-threatening factors

BARTÓK ANDRÁS

A KÍNAI NÉPKÖZTÁRSASÁG VÉDELEMPOLITIKÁJA 1989-TŐL NAPJAINKIG

A tanulmány célja bemutatni a KNK védelempolitikájának alakulását az 1989-et követő évtizedekben, főként a haderőfejlesztés és reformok tükrében. A történeti áttekintést követi a haderőnemek főbb eszközrendszereinek és szervezeti változásainak nyomon követése. Ennek fényében azonosítható a KNK védelempolitikai fejlődéstörténetének néhány fontosabb szakasza, melyek a modernizáció megalapozása, a Tajvan szigetével szembeni elrettentés kiépítése, az A2/AD képességek kiépítése, a tengeri „aktív védelem" eszközrendszereinek növelése. Ezen folyamat szerves folytatása lehet Kína globális erőkivetítési képességeinek fejlesztése, ennek nyomon követése, értékelése a további időszak feladata lesz majd.

Kulcsszavak: Kínai Népköztársaság, védelempolitika, haderőfejlesztés

BEDERNA ZSOLT

AZ ÁLTALÁNOS ADATVÉDELMI RENDELET ÉS AZ INFORMÁCIÓBIZTONSÁG KAPCSOLÓDÁSI PONTJAI

Az elmúlt egy-másfél évtizedben a személyes adatok gyűjtését és szervezetek közötti megosztását megvalósító tevékenységek száma jelentősen megemelkedett, amely indokolttá tette a vonatkozó jogszabályi környezet felülvizsgálatát és módosítását. Ennek következtében a felülvizsgálat 2012-ben megkezdődött, amely eredményeképp 2016. április 27-én lépett hatályba Általános adatvédelmi rendelet. A jogszabályban előírt kötelezettségeket 2018. május 25-től kötelezően alkalmazni szükséges, melyek jelentős mértékben összefonódnak az információbiztonsági irányítási rendszerrel, valamint a mindennapokban alkalmazott információbiztonsági kontrollokkal.

Kulcsszavak: információbiztonság, IBIR, általános adatvédelmi rendelet, GDPR

ANDRÁS BARTÓK

THE DEFENCE POLICY OF THE PEOPLE'S REPUBLIC OF CHINA SINCE 1989

The paper aims to give an overview of the PRC's defence policy, since 1989, focusing on the reforms and military development scheme of the armed forces. A historical overview is followed by a detailed look at the equipment and the organizational changes of the five armed services. A look at the major development projects helps us create a narrative of the military reform waves: 1. baseline modernization, 2. deterrence build-up against Taiwan, 3. A2/AD defensive build-up, 4. „active defence" at sea. A natural continuation of this process could be the build-up of China's global power projection capabilities, which should be the focus of future analysis.

Keywords: People's Republic of China, defence policy, military modernization

ZSOLT BEDERNA

CONNECTION POINTS OF GDPR AND INFORMATION SECURITY

In the last ten to fifteen years, the number of activities implementing the collection and sharing of personal data between organizations has increased considerably, causing the legislator to review and modify the relevant legal environment. As a consequence, the review began in 2012, which resulted in the General Data Protection Regulation on April 27, 2016. Its obligations shall be applied from May 25, 2018. The renewed data protection controls have huge amount of connection points with the information security management system, and therefore with the nowadays applied information security controls.

Keywords: information security, ISMS, General Data Protection Regulation, GDPR

FEKETE CSANÁD

HADVISELÉS AZ INFORMÁCIÓS KORSZAKBAN AZ ÚJ PARADIGMA KÜSZÖBÉN?

Az elmúlt évek eseményei az érdeklődés középpontjába állították az információs hadviselés kérdéskörét, amely korunk információs társadalmainak kialakulását követően az államok alapvető biztonsági fenyegetésévé lépett elő. Az információs környezet napjainkra egy olyan globális küzdőtérré változott, ahol az államok és államszint alatti szereplők folyamatos harcot vívnak egymással stratégiai érdekeik előmozdítása céljából. Publikációmban ennek figyelembevételével igyekszem átfogó képet nyújtani a konfliktusok információs tartományáról és a hadügyi forradalom aktuális kérdéseiről.

Kulcsszavak: információs hadviselés, jövő fegyveres konfliktusai, 21. századi hadviselés

DR. MÓGOR-KRÓZSER TERÉZIA

SZEMÉLYES ADATOK VÉDELMÉNEK FŐ FELADATAI AZ UNIÓS SZABÁLYOZÁS SZEMSZÖGÉBŐL

A publikáció rövid áttekintést ad az Európai Parlament és a Tanács 2016/679 rendelete (a továbbiakban: Rendelet/GDPR) bevezetésével, gyakorlati megvalósításával kapcsolatos kérdésekről. A cikk bemutatja a Rendelet által meghatározott változásokat, amelyek megvalósulása révén a természetes személyek személyes adataik kezelése és áramlása tekintetében a korábbinál szélesebb lehetőséget kapnak. A publikáció iránymutatást ad az adatkezelők, adatfeldolgozók részére a GDPR alkalmazásának előírásairól és lehetőségeiről.

A Rendelet 2016. május 25-én lépett hatályba, rendelkezéseit a kétéves felkészülési időszakot követően, 2018. május 25-től kell kötelezően alkalmazni. A GDPR az EU tagállamainak adatvédelmét hivatott közös nevezőre hozni, és láthatóan lehetőséget biztosít a vállalkozások és munkáltatók részére, hogy a szabályozással járó komplex és összetett feladatoknak meg tudjanak felelni. Az új jogszabály egyben hatályon kívül helyezte a 95/46/EK rendeletet.

Kulcsszavak: adatvédelem, személyes adatok, adatvédelmi szabályozás, adatkezelés, adatfeldolgozás, adatvédelmi tisztviselő

CSANÁD FEKETE

WARFARE IN THE INFORMATION AGE, THE DAWN OF A NEW PARADIGM?

The events of recent years put the issue of information warfare into the focus of attention, which after the emergence of information societies has become the fundamental security threat to the states. The information environment has now become a global arena where states and non-state actors are struggling with each other in order to achieve their strategic goals. In this paper, I will try to provide a comprehensive picture of these conflicts, and the current issues regarding the revolution in military affairs.

Keywords: Information warfare, future of armed conflicts, 21st century warfare

TERÉZIA MÓGOR-KRÓZSER DR.

MAIN DUTIES OF PROTECTING PERSONAL DATA FROM THE POINT OF VIEW OF EU REGULATION

The publication gives a brief overview of the questions with regard to the implementation and practical realisation of the Regulation of the European Parliament and of the Council No. 2016/679 (hereinafter: Regulation/GDPR). The article presents the changes defined in the GDPR which enable natural persons to manage and to flow their personal data in a broader scale. The publication provides guidance for the data controllers and for the data processors about the arrangements and possibilities of the GDPR's application.

The GDPR came into force on 25 May 2016, its provisions have to be applied as of 25 May 2018 following a preparatory period of two years. The GDPR appears to allow the entrepreneurs and employees to comply with their complex tasks related to the regulation. The new legislation also repeals the Regulation (EC) No. 95/46.

Keywords: data protection, personal data, data protection regulation, data management, data processing, data protection officer

OTTI CSABA – DR. KOLNHOFER-DERECSKEI ANITA

AZ EMBEREK ELFOGADÁSI KÜSZÖBE A BIOMETRIKUS RENDSZEREK MEGBÍZHATÓSÁGÁVAL SZEMBEN

Minden biztonsági beruházás egyik legfontosabb tényezője, hogy a felhasználók képesek és hajlandók-e megfelelően használni a rendszert. A biometrikus beléptetőrendszereknél ez fokozottan így van, mivel az algoritmusok valószínűségekkel dolgoznak és a felhasználók soha nem lehetnek biztosak abban, hogy 100%-os pontossággal ismeri fel őket. Ugyanakkor a biometrikus rendszerek gyártói által megadott értékek nem érhetőek el a valós alkalmazásokban, sőt a legtöbb esetben több nagyságrend eltérés van köztük. Publikációnkban bemutatjuk a legfrissebb kutatásunk eredményeit, amiben meghatározzuk a felhasználók beléptető rendszerek hibáival szemben mutatott egyéni szubjektív elfogadási küszöbét, ezáltal a biometrikus rendszerek felhasználói oldalról is értékelhetővé válnak.

Kulcsszavak: FRR, biometrikus beléptető rendszerek, felhasználók elfogadási küszöbe, fennakadás

DR. TÚRI VIKTÓRIA

A TERRORISTÁK PSZICHOLÓGIAI ÉS BIOLÓGIAI JELLEGZETESSÉGEI ÉS KIVÁLASZTÁSI MÓDSZEREI

A terrorizmus bár mindennapjaink részévé vált, mégis nehezen értelmezhetjük az elkövetők motivációit. Még nehezebb kérdés a terroristák pszichológiai motivációját feltérképezni. Mi motiválja őket, mennyire agresszívek?
Milyen kényszer, késztetés vagy motiváció veszi rá arra ezeket az embereket, hogy robbantsanak, hogy pusztítsanak? Tanulmányomban ezekre próbálok magyarázatot találni.

Kulcsszavak: lélek, motiváció, pszichológiai jellemzők, agresszió

CSABA OTTI – ANITA KOLNHOFER-DERECSKEI DR.

THE ACCEPTANCE THRESHOLD OF INDIVIDUALS REGARDING BIOMETRICAL SYSTEMS

One of the most important factors of any security investment is whether the users will be able and willing to use the system properly. In case of biometric access control systems, as algorithms operate with probabilities and the users can never be sure that they are recognized with a 100% accuracy. At the same time the error values provided by the manufacturers of biometric systems are not properly available or sometimes these are only algorithmic data. The aim of this study to provide the results of an empirical research and show the users' individual subjective acceptance regarding the errors of access control systems. Therefore, the biometric systems can be evaluated from the users' point of view.

Keywords: FRR, biometrics, user acceptance, failures

VIKTÓRIA TÚRI DR.

PSYCHOLOGICAL AND BIOLOGICAL CHARACTERISTICS AND TARGET SELECTION METHODS OF TERRORISTS

Although terrorism has become part of our daily lives, it is still difficult to interpret the motivation of the perpetrators. It is even more difficult to map the psychological motivations of a terrorist. What motivates them, how aggressive are they? What kind of urge, motivation or drive makes these people to blow something or somebody up and to destroy. The study aims to give an explanation to these answers.

Keywords: soul, motivation, psychological characteristics, aggression

CSEHI GÁBOR

AZ ASZIMMETRIKUS KONFLIKTUSOK ÉS AZ EGÉSZSÉGBIZTONSÁG

Az aszimmetrikus konfliktusok egy fontos terepe az egészségügy. A veszteségek egy része a nem megfelelően szervezett egészségügyi rendszer (ellátás, egészségügyi felderítés) következménye is lehet, amely a konfliktus sikeres megoldását veszélyeztetik. Fel kell készíteni a civil és katonai egészségügyi rendszereket az aszimmetrikus konfliktusokra. Az egészségbiztonság globális szinten védendő, melyre különböző mechanizmusok léteznek.

Kulcsszavak: aszimmetrikus konfliktusok, egészségügyi rendszer, járvány, egészségügyi válsághelyzet, pandémia, betegellátás, gyógyszergyártás, gyógyszer-ellátás, nozokomiális fertőzés, WHO, Nemzetközi Egészségügyi Rendszabályok

CSURGÓ ATTILA

A KATONAI MŰSZAKI TÁMOGATÁS AZ ASZIMMETRIKUS HADVISELÉS KORÁBAN, KÜLÖNÖS TEKINTETTEL AZ RÖGTÖNZÖTT ROBBANÓSZERKEZETEK ELLENI HARCRA

Az aszimmetria jelenléte a hadviselésben, folyamatosan megfigyelhető a hadtörténelemben korszakról-korszakra. Az új fegyverek, eljárások és módszerek megjelenése általában aszimmetriát teremtett a hadviselésben. A 20. századelején a műveleti eljárásokban a tüzérség és a harckocsik domináltak, míg a második felében a légierő.
Ugyanakkor a 21. században a szembenálló felek közötti jelentős technológiai különbség a konfliktusok elhúzódását eredményezte, amely az rögtönzött robbanószerkezetet tette a hadviselésre hatást gyakorló fegyverré. Az általa teremtett újszerű műveleti környezet, megítélésem szerint hatással van a műszaki támogatás feladatira is.

Kulcsszavak: hadviselés, aszimmetria, gerillaharc, műszaki támogatás, házilag készített robbanószerkezet

GÁBOR CSEHI

ASYMMETRIC WARFARE AND HEALTH SECURITY

Healthcare is an important area for Asymmetric conflict. Part of the losses might be the consequence of an inadequately organized healthcare system (health care, health monitoring) that endangers the successful resolution of the conflict. Civilian and military healthcare systems must be prepared for asymmetric conflicts. Health security needs to be protected on a global scale for which various mechanisms exist.

Keywords: Asymmetric Warfare, health system, pandemic, health crisis, health care, medicine supply, nosocomial infection, World Health Organization, International Health Regulations

ATTILA CSURGÓ

THE MILITARY ENGINEERING SUPPORT IN THE AGE OF ASYMMETRIC WARFARE, WITH SPECIAL FOCUS ON COUNTERING – IED.

The presence of asymmetry in warfare can be constantly observed from era to era in military history. The appearance of new weapons and methods created asymmetry in warfare. In the first half of the 20th century artillery and battle tanks dominated in operational procedures, while in the second half the air force. However in the 21st century, the significant technological gap between the opposing parties resulted in protracted conflicts, which made the improvised explosive device an effective weapon of warfare. The created new operational environment, in my opinion influences the tasks of the military engineer support.

Keywords: warfare, asymmetry, fight of guerrilla, engineering support, improvised explosive device

SZERZŐINK

Bartók András	NKE NETK Nemzetközi Kapcsolatok és Diplomácia Tanszék, tanársegéd
Bederna Zsolt	Óbudai Egyetem Biztonságtudományi Doktori Iskola, doktorandusz hallgató
Csehi Gábor	NKE Hadtudományi Doktori Iskola, doktorandusz hallgató
Csurgó Attila	ezredes, NKE Hadtudományi Doktori Iskola, doktorandusz hallgató
Fekete Csanád	NKE Nemzetközi és Európai Tanulmányok Kar, tanársegéd NKE HDI doktorandusz hallgató
Dr. Kassai Károly	ezredes, PhD, a KNBSZ munkatársa
Dr. Kolnhofer-Derecskei Anita	PhD, Óbudai Egyetem, Keleti Károly Gazdasági Kar, egyetemi adjunktus
Dr. László Viktória	NKE HHK Katonai Vezetőképző Intézet, tanársegéd
Dr. Mógor-Krózser Terézia	Nemzeti Közszolgálati Egyetem, HHK Szakmai Tanfolyami Központ
Nagyszegi Teréz	HM Védelempolitikai Főosztály
Otti Csaba	Óbudai Egyetem Biztonságtudományi Doktori Iskola, doktorandusz hallgató
Pozderka Gábor	HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség
Dr. habil. Resperger István	ezredes, PhD, NKE Nemzetbiztonsági Intézet, igazgató
Dr. Túri Viktória	Wekerle Sándor Üzleti Főiskola, főiskolai docens, szakszpichológus

E SZÁMUNKAT LEKTORÁLTÁK

Dr. Fürjes János	alezredes, PhD, a KNBSZ munkatársa
Dr. Kaiser Ferenc	PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék, tanszékvezető
Dr. Kenedli Tamás	ezredes, PhD, a KNBSZ munkatársa
Dr. Magyar Sándor	ezredes, PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék, adjunktus, a KNBSZ munkatársa
Dr. habil. Resperger István	ezredes, PhD, NKE Nemzetbiztonsági Intézet, igazgató
Prof. Dr. Rajnai Zoltán	PhD, Óbudai Egyetem Biztonságtudományi Doktori Iskola vezetője
Simon László	alezredes, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
Prof. Dr. Szternák György	nyá. ezredes, CSc, NKE egyetemi tanár

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[350] 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.

[350] 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.[351]

Példák:

ÁCS Tibor: A reformkor hadikultúrájáról, *Budapest, 2005, Zrínyi Kiadó. ISBN 963 9276 45 6*

BEREK Lajos: A hadtudományi kutatómunka alapjai, In: SZILÁGYI Tivadar (szerk.): Szemelvények, Budapest, 1994, Zrínyi Miklós Katonai Akadémia. pp. 31–50.

KOVÁCS Jenő: Az új magyar hadtudomány gyökerei, fejlődésének szemléleti problémái, In: Új Honvédségi Szemle, 1993. 47. évf. 6. sz. pp. 1–7. ISSN 1216-7436

Global Trend 2020: Mappingthe Global Future, http://www. foia.cia.gov/2020/2020.pdf (Letöltés ideje: 2012.08.21.),

Ábra, vázlat, térkép, diagram, egyéb melléklettel szembeni követelmények:

- az ábra, vázlat címe;
- az ábra, vázlat forrás (vagy: Szerkesztette: …);
- az ábra, vázlat sorszáma (pl. 1. ábra.);
- idegen nyelvű ábra, vázlat esetén lehetőség szerint magyar nyelvű jelmagyarázat.

Rövidítések, idegen kifejezésekkel kapcsolatos követelmények:

- az idegen kifejezéseket, rövidítéseket magyarul és eredeti idegen nyelven kell az írásműben az első alkalommal feloldani lábjegyzetben;

Példa:

- WFP – (World Food Program – ENSZ Világélelmezési Programja).

SZERKESZTŐBIZOTTSÁG

[351] Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. p. 18.