



**KATONAI NEMZETBIZTONSÁGI
SZOLGÁLAT**

XV. évfolyam 3. szám 2017. november

**SZAKMAI
SZEMLE**

ALAPÍTVÁ: 2003

BUDAPEST

**A Katonai Nemzetbiztonsági Szolgálat
tudományos-szakmai folyóirata**

Felelős kiadó

Kovács József altábornagy, főigazgató

Szerkesztőbizottság

Elnök:	Dr. Béres János, PhD	vezérőrnagy
Tagok:	Árpád Zoltán	ezredes
	Dr. Fürjes János Norbert, PhD	alezredes
	Dr. Kassai Károly, PhD	ezredes
	Dr. Kenedli Tamás, PhD	ezredes
	Dr. Magyar Sándor, PhD	ezredes
	dr. Sabjanics István	főhadnagy
	Szabó Károly	ezredes
	Tóth Csaba Mihály	alezredes
	Simon László	alezredes
	Dr. Vida Csaba, PhD	alezredes
Felelős szerkesztők:	Dr. Kenedli Tamás, PhD	ezredes
	Simon László	alezredes
Olvasószerkesztő:	Tóth Csaba Mihály	alezredes
Tördelő szerkesztő:	Szabó Beatrix	

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

BIZTONSÁG- ÉS VÉDELEMPOLITIKA

DR. FARKAS ÁDÁM A TERRORIZMUS ELLENI HARC, MINT KIEMELT ÁGAZATKÖZI FEGYVERES VÉDELMI FELADAT	5
SZENTIRMAI PÉTER AZ UKRÁN VÁLSÁG KATONAI OLDALÁNAK ÚJ KIHÍVÁSAI	21
CSER ORSOLYA A MAGYAR NEMZETI BANK HONVÉDELMI ÁGAZATI FELADATAI	45

TECHNIKAI RENDSZEREK

DEÁK VERONIKA BIZTONSÁGTUDATOSSÁG AZ INFORMÁCIÓS KÖRNYEZETBEN	59
GULYÁS ATTILA KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA I.	78
FINK NÁNDOR – HORVÁTH CSONGOR MÁRK A SZOLGÁLTATÓ ROBOTIKA HELYZETE ÉS KUTATÁSI IRÁNYAI	90

ALKALMAZOTT NEMZETBIZTONSÁGI-ELHÁRÍTÓ ISMERETEK

KOVÁCS KRISZTIÁN ALDRICH HAZEN AMES TÖRTÉNETE I.	113
--	-----

FÓRUM

DR. GYARAKI RÉKA JOGI SZABÁLYOZÁS A NEMZETI ELEKTRONIKUS ADATVAGYON, AZ AZT KEZELŐ INFORMÁCIÓS RENDSZEREK, LÉTFONTOSÁGÚ INFORMÁCIÓS RENDSZEREK ÉS RENDSZERELEMEK BIZTONSÁGÁRÓL	140
MAKAY MÁTYÁS A RACIONÁLIS GONDOLKODÁS KÉPESSÉGÉNEK KVANTITATÍV MÉRÉSE	155

AZ OLVASÓHOZ

DR. DÁVID FERENC A BIZTONSÁG ÉS NEMZETBIZTONSÁG MEGISMÉRÉSÉNEK SZÁLA: TUDOMÁNYOS-ISMERETTERJESZTŐ ELŐADÁSOK A „KUTATÓK ÉJSZAKÁJÁN”	175
E SZÁMUNK TARTALMA	178
CONTENTS	179
SZERZŐINK.....	188
E SZÁMUNK LEKTORAI	189
A PUBLIKÁLÁS FELTÉTELEI	190

DR. FARKAS ÁDÁM

A TERRORIZMUS ELLENI HARC, MINT KIEMELT ÁGAZATKÖZI FEGYVERES VÉDELMI FELADAT¹

"A terrorizmusra olyan támadások jellemzők, amelyek jellegükben kiméletlenek, a széles társadalomra gyakorolt hatásukat tekintve pedig kiszámíthatatlanok. [...] A terrorcselekmények olyan törvényeket szegnek meg, vagy olyan törvények megszegésére szőnek összeesküvést, amelyek a legtöbb társadalom számára közösek. [...] A terrorizmus nem politikai aktivizmus és nem »szabadságharc«. Tudatos döntés arról, hogy halálos taktikát választanak, mintegy kriminális szimbólum gyanánt, hogy egy ügy támogatására vagy népszerűsítésére rémületet, megfélemlítést és rettegést gerjesszenek."²

Marie-Helen Maras

A terrorizmus elleni harc az elmúlt évek Európájának aktuális, sokrétű, komplex és meglehetősen intenzív biztonsági kihívása,³ melyet a vérfagyasztó és világot bejáró képsorok, az emberéletek százában mérhető áldozatszám, valamint az állami reakció oldaláról a rendőri és katonai erők közös fellépése fémjelez. Egy olyan kihívásról beszélünk tehát, amely abban a pillanatban, hogy visszatérő támadásokkal lépett be az Európai gondolkörbe, azonnal ágazatközi jelleget öltött

¹ A mű a KÖFOP-2.1.2-VEKOP-15-2016- 00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Concha Győző Doktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

² Marie-Helen MARAS: A terrorizmus elmélete és gyakorlata. Budapest, Antall József Tudásközpont, 2016, p. 31.

³ Ez a kihívás és egyben feladat rendkívül sokrétű, mivel maga a terrorizmus is egy rendkívül sokrétű és komplex problémahalmaz, melynek kiismerése, kezelhetősége tekintetében is folyamatos a kutatói, szakirodalmi hiánypótlás. E körből példaként lásd: Marie-Helen MARAS i.m. (2016), TÁLAS Péter (szerk.): A terrorizmus anatómiája. Budapest, Zrínyi Kiadó, 2006., KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus. Budapest, Zrínyi kiadó, 2016., Jonathan BARKER: A terrorizmus. Budapest, HVG kiadó, 2003., Charles TOWNSHEND: Terrorizmus. Budapest, Magyar Világ Kiadó, 2003., STEWART Gail B.: Terrorism. San Diego, Kidhaven Press, 2002., TAYLOR Robert: History of Terrorism. San Diego, Lucent Books, 2002., EGENDORF Laura K. (ed.): Terrorism: opposing viewpoints. San Diego, Greenhaven Press, 2004., Ekaterina STEPANOVA: Terrorism in asymmetrical conflict. Ideological and Structural Aspects. Oxford, Oxford University Press, 2008., RESPERGER István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői. In Hadtudomány 2010/4. szám, pp. 68-77., SIMICSKÓ István: A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével. In Hadtudomány 2016/3-4. szám, pp. 100-113.

az állami fellépés szempontjából. Ezt példázva Franciaország, Belgium és Olaszország is szükségét látta annak, hogy katonai egységekkel erősítse meg a közrendvédelmet a kiemelt közterületeken, de megjegyyezhető, hogy erre törvényben biztosított lehetőség van az Egyesült Királyságban is.

Ezzel Európában látványos változás következett be a terrorizmus elleni harc tekintetében még annak ellenére is, hogy Nyugat-Európában messze nem minősül olyan jellegű tabunak, vagy „eretnek gondolatnak” a katonai erő belföldi, különleges jogrend nélküli, rendészeti célú igénybevétele, mint ahogy ez Közép-Európa diktatúrákat megélt államaiban jellemző.

Ez a fordulat nem teljesen újszerű, messze nem előzmények nélküli és egyáltalán nem jelenti azt, hogy bárhol is vitatnák a terrorizmus elleni fellépés alapvetően rendészeti és nemzetbiztonsági jellegét. A fordulat egyrészt abban ragadható meg, hogy az államok felismerték azt, hogy ezzel a fenyegetéssel szemben is alkalmazandó az erőfelmutatás és a nagyláthatóságú jelenlét elve, másrészt pedig azt, hogy a béketeremtő és békefenntartó missziókra alkalmazott, bukott államokban műveleteket végrehajtó hadseregek quasi rendészeti tapasztalatai a megfelelő továbbképzésekkel transzformálhatók a honi igénybevételre, harmadrészt pedig hogy egyértelműnek tűnnek az Iszlám Állam elnevezésű terrorszervezet⁴ felívelése óta a katonai műveletekkel érintett területek és az onnan „exportált” terrortámadások közti összefüggések.

Kérdés azonban, hogy megáll-e itt az ágazatközi jelleg erősítése, ahogy az is, hogy kell-e gondolkodni a terrorizmus elleni intézmények önállósításában, vagy sajátos karakterük tovább erősítésében? Hasonló kérdés az is, hogy a fegyveres erők bevonása milyen további ágazatközi kooperációkra nyithat kaput a jövőben, s hogy ezekkel miként erősíthető az európai államok biztonsága?

⁴ Már önmagában az is rögzítendő, hogy az Iszlám Állam elnevezésű terrorszervezet működésére nézve számos kötet született ugyan az elmúlt években, de még messze állunk attól, hogy kimerítően feltártnak tekinthetnénk az „Iszlám Állam kérdést”, illetve annak ösztönző hatásait más terrorista szervezetekre és a terrorizmus jövőbeni alakulására. Ezen ismeretek birtoklása nélkül pedig a védelem szempontjából a védelmi lehetőségek kialakításakor igenis élni kell a „worst case scenarióra”, a legrosszabb forgatókönyvre készülés eszközével. Az Iszlám Állam elnevezésű terrorszervezet vonatkozásában lásd: Kenneth KATZMAN – Christopher M. BLANCHARD – Clara E. HUMUD – Rhoda MARGESSON – Matthew C. WEED: The „Islamic State” Crisis and U.S. Policy. Washington, Congressional Research Service, 2015. KIS-BENEDEK József: Az Iszlám Kalifátus és a globális dzsihád új tendenciái. In Hadtudomány 2014/3-4. szám, pp. 22-33. N. RÓZSA Erzsébet: Az Iszlám Állam előretörése Irakban és az amerikai válaszcsepások. In Nemzet és Biztonság 2014/4. szám, pp. 56-61.; SELJÁN Péter: Harc az Iszlám Állam ellen. In Nemzet és Biztonság 2014/5. szám, pp. 63-74.; ARANY Anett – N. RÓZSA Erzsébet – SZALAI Máté: Az Iszlám Állam – következmények. Budapest, Külügyi és Külgazdasági Intézet KKI-tanulmányok T-2015/1, 2015. Loretta NAPOLEONI: Az iszlamista főnix, Az Iszlám Állam születése és a Közel-Kelet újrafelosztása. Budapest, HVG kiadó, 2015. Michael WEISS – Hassan HASSAN: Az Iszlám Állam. A terror hadserege belülről. Budapest, HVG kiadó, 2015. BESENYŐ János – PRANTNER Zoltán – SPIEDL Bianka – VOGEL Dávid: Iszlám Állam. Terrorizmus 2.0. Történet, ideológia, propaganda. Budapest, Honvéd Vezérkar Tudományos Kutatóhely – Kossuth kiadó, 2016.

Ehhez a változtatási folyamathoz az Alaptörvény hatodik módosításával és a Magyar Honvédségnek a FINA világbajnokság védelmébe történő bevonásával⁵ Magyarország is elkezdett felzárkózni. Érdemes azonban áttekinteni, hogy ezen felzárkózási folyamat milyen kérdéseket vet fel és milyen további teendőket irányoz elő a szabályozás terén. Jelen tanulmány keretei között ezért arra teszek kísérletet, hogy a változási folyamat rövid áttekintése után néhány támponttal szolgáljak a terrorizmus elleni fellépés ágazatközi jellegének hazai erősítéséhez, finomhangolásához.

1. A jelenlegi szabályozás előzményei és sarokpontjai

A terrorizmus elleni fellépés alapvető belügyi jellege még az államszocialista időszakban sem volt kérdéses. A tény, hogy a terrorizmus elleni operatív eszközökkel történő fellépés intézményesített alapját a Belügyminisztérium III/II. Csoportfőnökség 8. osztályán belül hozták létre az 1970-es évek végén, s nem sokkal később már önálló 10. osztállyá szervezve működtették, ezt megfelelően tükrözi.⁶ Ez a fajta „tradíció” a nemzetbiztonsági szektorban a mai napig fennmaradt, hiszen úgy az állambiztonsági szervek, mint a rendszerváltást követően a nemzetbiztonsági szolgálatok – egészen napjainkig – feladatrendszerükben tudják a terrorizmus elleni fellépés nemzetbiztonsági vonatkozásait.⁷ Ebben a tendenciában újszerű, az információelemzést hangsúlyozó szemléletet, de egyben a nemzetbiztonsági szolgálatok rendszerében korántsem problémamentes megoldást tükröz a Szervezett Bűnözés Elleni Koordinációs Központ bázisán létesített, de már nemzetbiztonsági szolgálatként törvényesített Terrorelhárítási Információs és Bűnügyi Elemző Központ – azaz a TIBEK – létrehozása.⁸

Szintén a belügyi feladatba tartozást mutatja, hogy a terrorizmussal szembeni műveleti fellépés a rendőrség keretei között, a Rendőri Ezredben került megszervezésre a rendszerváltozást megelőzően, előbb decentralizált szakaszokkal, utóbb pedig a Komondor Terrorelhárító Szolgálatba történő centralizálással. Erre a szisztémára épült az a változás, hogy a rendszerváltozást követően önállóan működő, országos hatáskörű szervként hozták létre a Rendőrség Különleges

⁵ A Magyar Honvédség által védendő létesítmények kijelöléséről, valamint a magyar állam folytonosságát és függetlenségét megtestesítő ereklyék köréről és az őrzésükre vonatkozó szabályokról szóló 78/2011. (V. 12.) Korm. rendelet 1. melléklete ugyanis a Honvédség által védendő létesítmények körébe sorolja hatályos szövege szerint a világbajnokság létesítményeit.

⁶ Vö.: BEKE József – DR. HEGYES Gabriella: A terrorelhárítás kezdetei Magyarországon – A C-79-es dosszié. In (T)Error & elhárítás 2015/I. szám. http://tek.gov.hu/tt_pdf/2015/bekedrhegyes.pdf (Letöltés ideje: 2017. 05. 25.) A BM III: főcsoportfőnökség feladatrendszere tekintetében bővebben lásd: A Magyar Népköztársaság belügyminiszterének 26/1979. számú parancsa a BM III. (Állambiztonsági) Főcsoportfőnökség Ügyrendjének kiadásáról.

⁷ Erre példákat is ad a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) a 4. § c) pontjában az Információs Hivatal, valamint 6. § h), ma) és mb) pontjaiban a Katonai Nemzetbiztonsági Szolgálatok tekintetében.

⁸ A TIBEK-et az európai terrorhullámra adott válaszként megalkotott, a békeidejű terrorellenes szabályozásfejlesztésére irányuló törvény iktatta be a magyar jog- és államrendszerbe. E tekintetben lásd a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény rendelkezéseit.

Szolgálatát, majd 1998-ban azt – mintegy visszalépésként – Terrorelhárító Szolgálatként beolvasztották a Készenléti Rendőrségbe.⁹ Ebbe a sorba illeszkedett a rendőrségi törvényben szabályozott, sajátos jogállású, önálló, országos hatáskörű rendőrség-típusként 2010-ben létrehozott Terrorelhárítási Központ (TEK), amely a belügyminiszter közvetlen alárendeltségében teljesíti feladatait és működésében néhol ötvözi a nemzetbiztonsági szférára jellemző jogositványokat a rendőrség korábbi különleges műveleti képességeinek feladatrendszerével.

Az operatív és a műveleti fellépés mellett a jog oldaláról értelemszerűen a terrorizmus elleni fellépés fő eszközét a büntetőjog jelentette, amelynek a vonatkozó szabályrendszerét jelentős mértékben bővítette a 2001. szeptember 11-ét követő európai jogharmonizációs törekvés a terrorizmus elleni fellépés körében, büntetőjogi eszközöket is kapcsolva a terrorizmus finanszírozásának pénzügyi jogi eszközrendszeréhez. Azt is mondhatnánk, hogy Magyarország tekintetében a kétezres évek terrorhullámát követően egyrészt az Amerikai Egyesült Államok által kezdeményezett műveletekben való katonai részvétel,¹⁰ másrészt pedig a büntetőjogi eszközrendszer fejlesztése¹¹ jelentette a változás fő irányát.¹² Arra vonatkozó törekvés, hogy a Magyar Honvédség valamilyen formában részt vehessen a terrorizmus elleni honi feladatokban, vagy hogy a terrorizmussal összefüggésben különleges jogrendi szabályozásra lenne szükség, ekkor még nem merült fel.

A 2015-ben kiújuló európai terrortámadások és az, hogy több nyugat-európai államban is ezerszám vezényeltek katonákat a közterületekre a rendőrség támogatása érdekében, valamint az, hogy 2015. november 13-a és 2017. október 31-

⁹ A témával kapcsolatban lásd: Hegedűs Ernő: Terrorelhárító erők szervezése a rendvédelmi szervezeteknél és a légi deszant csapatoknál. In Rendvédelem-történeti füzetek 2010/22. szám, pp. 53-59.

¹⁰ A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény az Amerikai Egyesült Államok szövetségi igényeire figyelemmel, de a katonai erők bevonása felé történő nyitásként megjelenítette a nemzetközi terrorizmus elleni fellépést a Magyar Honvédség feladatrendszerében. A 70. § (1) bekezdés c) pontja szerint a Magyar Honvédség feladat volt a „közreműködés az arra kijelölt és felkészített erőkkel a nemzetközi terrorizmus elleni harc katonai feladatainak ellátásában.”

¹¹ Ezt példázzák: a terrorizmus elleni küzdelemről, a pénzmosás megakadályozásáról szóló rendelkezések szigorításáról, valamint az egyes korlátozó intézkedések elrendeléséről szóló 2001. évi LXXXIII. törvény, a robbantásos terrorizmus visszaszorításáról, New Yorkban, az Egyesült Nemzetek Közgyűlésének 52. ülészakán, 1997. december 15-én elfogadott nemzetközi egyezmény kihirdetéséről szóló 2002. évi XXV. törvény, a terrorizmus finanszírozásának visszaszorításáról, New Yorkban, az Egyesült Nemzetek Közgyűlésének 54. ülészakán, 1999. december 9-én elfogadott nemzetközi Egyezmény kihirdetéséről szóló 2002. évi LIX. törvény, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2007. évi CXXXVI. törvény, vagy például az Európa Tanács terrorizmus megelőzéséről szóló, Varsóban, 2005. május 16-án kelt Egyezménye kihirdetéséről szóló 2011. évi II. törvény.

¹² Ennek szakirodalmából lásd: BARTKÓ Róbert: A terrorizmus elleni küzdelem kriminálpolitikai kérdései. Győr, Universitas-Győr Nonprofit Kft., 2011., PÓCZIK Szilveszter: Bevezetés a terrorizmus kriminológiájába I. rész. Definíció, tipológia, jog és történelem. In IRK Ferenc (szerk.): Kriminológiai Tanulmányok 43. Budapest, Országos Kriminológiai Intézet, 2006, pp. 63-94., PÓCZIK Szilveszter: A terrorizmus kriminológiai perspektívában. In Rendészeti Szemle. 2006/9. szám pp. 45-59., HAVASI Zoltán: A terrorizmus és a jog. In Nemzetvédelmi Egyetemi Közlemények 2003/4. szám pp. 46-68.

e között Franciaországban rendkívüli állapot volt érvényben,¹³ újragondolás tárgyává tette a terrorizmus elleni fellépés eszközrendszerét és szabályozási kereteit hazánkban. Ennek a folyamatnak két vonulata volt. Az egyik a békeidejű eszközök finomítása, fejlesztése a Belügyminisztérium előkészítésében, a másik pedig az Alaptörvény hatodik módosításának előkészítése a Honvédelmi Minisztérium gondozásában.¹⁴ A szabályozás eredménye egyrészt a rendőri, nemzetbiztonsági eszközpark és intézményrendszer fejlesztése lett, amelyhez kapcsolódott a terrorizmus elleni küzdelem feladatainak egységes végrehajtási rendjéről szóló 1824/2015. (XI. 19.) Korm. határozat megalkotása is. Ezt a békeidejű válságkezelésre hivatott szabályozási törekvést egészítette ki a közjogi értelemben vett „ultima ratio” jellegű eszközzel az Alaptörvény hatodik módosítása és általa a közvetlen és jelentős terrorfenyegetettség, vagy megtörtént terrortámadás esetén bevezethető terrorveszélyhelyzet beiktatása az Alaptörvény 51/A. cikkével a különleges jogrendek körébe. A kétirányú szabályozás célja egy a normál jogrendtől a különleges jogrendig terjedő eszközpark biztosítása volt, valamint az utóbbi tekintetében a rendkívüli intézkedések bevezethetőségének lehetővé tétele és a Magyar Honvédség felhasználásának megalapozása az erre vonatkozó közjogi döntés alapján.

Az így kialakított szisztéma ugyan jelentős fejlesztésként értékelendő a korábbi szakaszos és részleges változtatásokhoz képest, de azzal kapcsolatban több kérdés és korrekciós igény is felvethető, aminek fő oka egyrészt a terrortámadások hatásával keletkező időprés lehet, másrészt pedig a szabályozás sajátosságai a különleges jogrendi elemek tekintetében. A kérdéses vonatkozások egyik nagy támpontját a terrorfokozatok, vagy riasztási szintek kérdése és az 1824/2015. (XI. 19.) Korm. határozat szabályozása adja, a másikat pedig a Magyar Honvédség és a rendészeti szervek terrorveszélyhelyzettel összefüggő kooperációjának további szabályozási igénye.

Az 1824/2015. (XI. 19.) Korm. határozat tekintetében láttatni szükséges, hogy az az Alaptörvény hatodik módosítása előtt született és a 2017. július 1-jén hatályos változata szerint sem szerepel benne a terrorveszélyhelyzetre történő utalás, holott a terrorszintek tekintetében a magas és a kritikus szint egyértelműen átfedéseket mutat a terrorveszélyhelyzet bevezethetőségének körülményeivel. A terrorveszélyhelyzetre való reflexió hiányával hozható összefüggésbe az is, hogy a határozat szervezeti hatályát nem terjesztette ki a jogalkotó a Magyar Honvédségre, holott az a terrorfokozatok kormányzati szinten vett általános bevezetése, majd az Alaptörvény hatodik módosítását követően már az esetleges felhasználásra való felkészülés miatt egyértelműen indokolt lett volna. Miközben tehát az 1824/2015. (XI. 19.) Korm.

¹³ A franciaországi rendkívüli állapot 2017. november 1-jén feloldásra került. Lásd: http://hvg.hu/vilag/20171030_Veget_er_Franciaorszagban_a_rendkivuli_allapot (Letöltés ideje: 2017. 10. 30.)

¹⁴ Maga a javaslat, illetve gondolat nem előzmények nélküli. Korábbi kutatásaim alapján magam is fogalmaztam meg ez irányba mutató javaslatot. E tekintetben lásd: FARKAS Ádám: Tévelygések fogságában? Tanulmányok az állam fegyveres védelmének egyes jogtani és államtani kérdéseiről, különös tekintettel Magyarországon katonai védelmére. Budapest, Magyar Katonai Jog és Hádijogi Társaság, 2016., FARKAS Ádám: Szemléletváltást védelmi aspektusban! In Pázmány Law Working Papers 2015/18. szám. http://d18wh0wf8v71m4.cloudfront.net/docs/wp/2015/2015-18_Farkas_.pdf (Letöltés ideje: 2017. 05. 25.)

határozat címe és tartalma alapján is abból a célból született hat nappal a párizsi terrortámadások után, hogy egységesítse a terrorizmus elleni küzdelem feladatainak kormányzati alárendeltségű ellátását, aközben ebből a körből lényegében kihagyta a Magyar Honvédséget, majd az Alaptörvény hatodik módosítását követően azokat a további szabályozási tárgyköröket, amelyek az azonnali reagálás érdekében egy esetleges terrorveszélyhelyzet kihirdetésének kezdeményezése, vagy annak előkészítése esetén szükségesek lehetnek. E körben külön kiemelendő, hogy a riasztási fokozatok tekintetében a határozat lehető legszélesebb körű hatályának meghatározása előmozdíthatta volna a különböző riasztási szisztémák összehangolását, különös tekintettel például arra, hogy Magyarország magára nézve elfogadta például a NATO Válságreagálási Rendszerét, melynek intézkedésgyűjteménye szintén tartalmaz egyfajta riasztási szisztémát,¹⁵ amivel az 1824/2015. (XI. 19.) Korm. határozat összhangjának kialakítása nem történt meg az elmúlt időszakban.

Ami a rendészeti szervek és a Magyar Honvédség közti kooperációt különösen a felhasználás témakörében illeti, az egy nagyobb súlyú eldöntendő kérdésből, valamint több részletszabályozási igényből tevődik össze. Egyrészt eldöntendő alapkérdés, hogy a felhasználás részletszabályait az intézkedési jogkör, a feladatellátás, a műveleti igénytámasztás, vagy épp a kényszerítő eszközök tekintetében a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvényben (a továbbiakban: Hvt.) kell-e rendezni, ahogy az a Magyar Honvédségnek a tömeges bevándorlás okozta válsághelyzet kezelésében való közreműködése kapcsán történt, vagy pedig az Alaptörvény 51/A. cikkének felhatalmazásaira figyelemmel egy különleges jogrendi kormányrendeletben. Az előbbi megoldás fő jellemzője az lenne, hogy bár előre átlátható és megismerhető szabályozást adna, de az esetleges szakmai módosítási igényeket a sarkalatos törvényi jelleg valamelyest korlátozná, vagy legalábbis egy rendkívüli intézkedéssel történő módosítás esetén szakmailag megkérdőjelezhetővé tenné. Az utóbbi megoldás fő jellemzője, hogy az ugyan rugalmas keret-meghatározást tesz lehetővé, ami akár a konkrét biztonsági helyzet sajátosságaihoz is igazíthatja különösen az intézkedésekre, illetve a rendészeti kényszerítő eszközök honvédségi alkalmazására vonatkozó szabályokat, azonban nem lenne előre átlátható és felvetheti a kérdést, hogy ezt nem kell-e törvényi szinten szabályozni azt megelőzően, hogy egy különleges jogrendi, tehát törvénytől – és egyben esetleg törvényrontó – rendeletbe iktatjuk a szükség óráján.

¹⁵ A témával kapcsolatban lásd: Hvt. 21.§ (1) bekezdés h) pontját és 64. § (1) bekezdését, valamint a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről szóló 278/2011. (XII. 20.) Korm. rendeletet és a NATO Válságreagálási Rendszerrel összhangban álló Nemzeti Intézkedési Rendszer működtetésével kapcsolatos feladatokról szóló 20/2014. (III. 21.) HM utasítást. Lásd továbbá: KESZELY László: A NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer alkalmazásának tapasztalatai az ukrán válsággal összefüggésben. In Hadtudomány 2015/1-2. szám, pp. 120-125., KESZELY László: A NATO válságreagálási rendszerével összhangban álló nemzeti intézkedési rendszer és a különleges jogrend összefüggései. In Katonai jogi és hadijogi szemle, 2014/1. szám, pp. 191-221.

A felhasználás, illetve a rendészeti szervek és a Honvédség közti együttműködés további szabályozási igényének egyik sarokpontját azoknak a részletszabályoknak a megadása adja, amely a felhasználás különös – törvényi, vagy különleges jogrendi kormányrendeleti szintű – szabályainak megadását követően válik lehetővé. E körbe sorolnám például a riasztási fokozatok összehangolását a sajátos katonai fokozati rendszerekkel, valamint egy BM-HM közös utasítás kiadását a műveleti együttműködés részletszabályairól.

Összességében tehát az látható, hogy a terrorizmus elleni szervezett állami fellépés intézmény- és szabályrendszere a 20. század második fele óta folyamatos változásban, bővülésben, fejlődésben van. Ennek eredményeként már kialakult egy meglehetősen komplex szisztéma, amely magában foglalja az operatív feladatok nemzetbiztonsági ellátását, a műveleti feladatok önállóított rendészeti ellátását, a büntetőjogi eszközszer meg erősítését, a terrorveszélyhelyzet különleges jogrendként történő bevezethetőségével a rendkívüli intézkedések bevezetésének lehetőségét, valamint a Magyar Honvédség esetleges különleges jogrendi felhasználását is.¹⁶ Ezen szisztémán azonban még bizonyos korrekciók szükségesek rövidtávon, valamint további módosítások mérlegelése is megfontolt hosszú távon, mivel jól látható, hogy a tág értelemben vett terrorizmus által jelentett kihívás nem csak az iszlamista nemzetközi terrorizmus keretei között, hanem akár a hibrid hadviselés vonatkozásában is értelmezhető és ezért további megerősítő intézkedéseket tesz szükségessé. Érdemes ezért a lehetséges fejlesztési irányokat a következőkben áttekinteni.

2. Lehetséges fejlesztési irányok a terrorizmus elleni fellépés ágazatközi vonatkozásaiban

A fent leírtakra figyelemmel a terrorizmus elleni fellépés ágazatközi vonatkozásainak tovább erősítése, valamint a meglévő szabályozás pontosítása érdekében szükségesnek mutatkozik a következő fejlesztési irányok mérlegelése:

- a) A terrorizmus elleni küzdelem feladatainak egységes végrehajtási rendjéről szóló 1824/2015. (XI. 19.) Korm. határozat módosítása;
- b) A Magyar Honvédség felhasználásának szabályozása, jogszabályi szintű és belső szabályozói szintű részletezése;
- c) A terrorizmust elhárító szerv jogállásának felülvizsgálata;

¹⁶ Magam csak fenntartásokkal érzem idetartozónak a Magyar Honvédség által védendő létesítmények kijelöléséről, valamint a magyar állam folytonosságát és függetlenségét megtestesítő ereklyék köréről és az őrzésükre vonatkozó szabályokról szóló 78/2011. (V. 12.) Korm. rendelet 2017. július 11-től hatályos módosítását, amely az 1. melléklet szerint beiktatta a Magyar Honvédség által védendő létesítmények körébe a Budapesten megrendezendő Úszó-, Vízilabda-, Múgró, Múúzó és Nyíltvízi Világbajnokság megvalósításához szükséges létesítményfejlesztésről szóló 2015. évi XXXIII. törvény hatálya alá tartozó létesítményeket. Ez ugyanis egyértelműen összefügg az európai terrorfenyegetettséggel, azonban maga a Korm. rendelet a Hvt. 36. § (1) bekezdés b) és e) pontjai szerinti feladatra irányuló felhatalmazás alapján áll, ami lényegesen szélesebb kört ölelhet fel a feladatrendszer tekintetében, azaz számos más biztonsági kihívás vonatkozásában is alkalmazható a létesítmények védelme kapcsán, ami azonban nem egyenlő tartalmilag a közrendvédelemben történő közreműködéssel, vagy az objektumok körén túlmutatóan a rendezvény közrendészeti, vagy terrorellenes biztosításával.

d) A katonai értelemben vett terrorellenes műveletek, illetve a bukott államok vonatkozásában végzett béketeremtő és békefenntartó műveletek egyes hozadékaiknak az összekapcsolása a tömeges bevándorlás okozta válsághelyzet kezelésével és a honi területen történő terrorizmus ellenes fellépéssel.

A 1824/2015. (XI.19.) Korm. határozat módosítása tekintetében alapvető fontosságúnak tartom, hogy az egyrésztől hatályában kiterjedjen a Magyar Honvédségre is, tartalmában pedig egyértelműen reflektáljon a terrorveszélyhelyzet bevezetésének lehetőségére, illetve ennek előkészítésére. E körben tehát szükséges a határozat első pontjában szereplő felsorolás kiegészítése a Magyar Honvédséggel, mivel ez a módosítás erősíteni tudja a határozat címe szerinti azon törekvést, hogy az abban meghatározott feladatok és riasztási szintek a terrorizmus elleni feladatok egységes végrehajtása felé vigyék a Kormány alárendeltségében működő és a feladatellátásban érintett szervezeteket.

Megfontolandónak tartom emellett azt is megvizsgálni, hogy a 3. alcímhez tartozó szabályok körében megjelenjen egy olyan kötelező szabály, amely a terrorveszélyhelyzet kihirdetésének kezdeményezésétől kezdődően mérlegelést nem tűrő módon teszi kötelezővé legalább a súlyos, illetve a kritikus fokozat bevezetését, mivel meglátásom szerint a riasztási fokozatok leírása alapján ezek a fokozatok egyértelműen fennállnak az Alaptörvény 51/A. cikke szerinti különleges jogrend kihirdetésének kezdeményezhetősége esetén.

Figyelemmel arra, hogy a határozat elfogadását követően megszületett az Alaptörvény hatodik módosítása, amely a Magyar Honvédség tekintetében jelentős és bizonyos előkészületeket mindenképp igénylő feladatként jelenítette meg a felhasználás lehetőségét, fontosnak tartom a határozat 7. alcímében egy olyan szabály megjelenítését, amely szerint a Magyarországot érintő közvetlen és jelentős terrorfenyegetettség, vagy elkövetett terrorcselekmény vonatkozásában a BM ügyelet azonnal tájékoztatja a Magyar Honvédség Központi Ügyeletét az esetleges felhasználás hatékony előkészíthetősége érdekében.

Mindezek felül az Alaptörvény hatodik módosítása miatt úgy gondolom, hogy szükséges volna egy új alcím keretében különös szabályokat meghatározni a súlyos és a kritikus fokozatok bevezetésével, valamint a terrorveszélyhelyzettel összefüggő különös szabályok biztosítása érdekében. E körben egyrészt megfontolandó lenne, hogy megerősítést nyerjen a Terrorellenes Koordinációs Bizottság a rendőri, katonai, nemzetbiztonsági közös műveletek koordinációja, műveletirányítással összefüggő közvetlen igénytámasztása, valamint a további szakmai szintű igények közvetlen támasztása terén. Ennek keretében természetesen

- a TKB nem venné át a műveletvezetés feladatait, de
- különösen a terrorveszélyhelyzet idején lényegében főszabállyá lépne elő az az egyébként kivételes eset, hogy a TKB közvetlenül tart kapcsolatot a belügyi ágazattól eltérő miniszterek alárendeltségébe tartozó szervezetekkel a miniszterek egyidejű értesítése mellett, valamint
- mérlegelést nem tűrő kötelezettségként jelenne meg az egyes ágazati szervek tekintetében a vonatkozó ügyeleti szolgálataik útján a műveletirányításhoz, illetve vezetéshez szükséges központjaik, továbbá az e célra kijelölt készenléti erők azonnali aktiválása.

A Magyar Honvédség felhasználására vonatkozó szabályozás kérdése meglátásom szerint a jogszabályi szinten egy hosszú távon eldöntendő kérdés, amely két lépcsős megoldást feltételez. A hatályos szabályozás azon rendszere, miszerint a Hvt. a felhasználásnak a lényegét és az Alaptörvény szerinti esetköreit határozza meg, nem szabályozási hiba, hanem a rendszerváltozás óta meglévő szabályozási tradíció fenntartása. E körben a jogalkotó sosem adta meg előzetesen azokat a részletszabályokat a törvényben, amelyek a bevont erők, eszközök és ezekkel összefüggő közjogi jelentések körén túli tárgykörökben szükségesek. Ennek oka egyrészt az lehet, hogy az eredetileg szükségállapot idején felmerülő felhasználás karakterisztikáját nagyban befolyásolhatja, hogy milyen konkrét körülmények kapcsán rendelték el a Honvédség ezen fellépését. Ezt a komplexitást tovább fokozta az a változás, hogy a terrorveszélyhelyzettel a szükségállapotnak is lett „előszoba tényállása” és ebben a felhasználás lehetősége is megjelent.¹⁷ Ezen tradíció alapvetése tehát az, hogy a Magyar Honvédség lényegében rendészeti jellegű feladatellátásának a Hvt. szabályaitól eltérő részletes intézkedési és kényszerítő eszköz alkalmazási rendelkezéseit szükség esetén, a konkrét körülmények figyelembevételével, közvetlenül az Alaptörvényben lévő azon felhatalmazás alapján lehet rendkívüli intézkedésként kormányrendeletben bevezetni, hogy a kihirdetés kezdeményezését követően a Kormány jogosult a Magyar Honvédség, a rendvédelmi szervek és a nemzetbiztonsági szolgálatok szervezetét, működését és tevékenysége ellátását érintő törvényektől eltérő intézkedések bevezetésére. Ennek a kizárólag különleges jogrend kihirdetésének kezdeményezésekor hatályba léptethető rendkívüli rendeletnek a folyamatos felülvizsgálata és naprakészen tartása tehát a rövid távú megoldás.

A felhasználás hosszabb távon mérlegelhető szabályozási megoldása az lehet, hogy a Hvt. átfogó felülvizsgálatával, vagy egy új Hvt. megalkotásával összefüggésben a felhasználás fent megjelölt szabályozási tárgyköreit a lehetséges esetkörök szerinti opcionális megoldások nyitva tartása mellett már előzetesen és nyilvánosan a sarkalatos törvény keretei között adja meg a jogalkotó, úgy ahogy ezt a tömeges bevándorlás okozta válsághelyzet vonatkozásában tette. Ez a megoldás egyrészt az előreláthatóság és megismerhetőség érdekében szakítana a rendszerváltozás óta fenntartott megengedő hallgatás gyakorlatával, másrészt azonban szükségessé tenné egy új rendszerű honvédelmi törvény megalkotását, mivel ez a fajta szellemiségváltás több más tárgykör szabályozása kapcsán is felmerülhetne igényként a Hvt. tekintetében. Egy ilyen jellegű átfogó módosítás, vagy egy új Hvt. megalkotása tehát csak hosszú távú megoldásként mérlegelhető.

A jogszabályi szint alatt, tehát elsősorban a közjogi szervezetszabályozó eszközök körében megjelenő szabályozási igények tekintetében szükségesnek mutatkozik, hogy hasonlóan a Magyar Honvédségnek a rendőrségi feladatok ellátásában történő közreműködése rendjéről szóló 25/2015. (IX. 14.) BM–HM együttes utasításhoz, megalkotásra kerüljön a felhasználás jogszabályi szintű kereteinek megadását követően egy olyan együttes utasítás, amely a végrehajtás igényeihez igazodó további részletszabályokat határozná meg.

¹⁷ A témáról bővebben lásd: FARKAS Ádám: Gondolatok a terrorveszélyhelyzetről. In Szakmai Szemle 2016/3. szám, pp. 174-189.

Ennek keretei között szükségesnek látom a feladat jellegéből adódó azonnali reagálás biztosítása érdekében legalább:

- a műveletirányítás közössé tételére, vagy fokozott összehangolására vonatkozó,
- a műveleti igények meghatározására,
- a közös járőrözésre és további védelmi feladatellátásra,
- az egyes rendkívüli intézkedések foganatosítására, valamint
- a különleges műveleti erők igénybevételére vonatkozó szabályok megadását.

Egy ilyen szabályozás után ugyanis egyértelműen és jól meghatározott kritériumok szerint hajtható végre a szükséges erők és a feladatellátás tervezése, illetve a meglévő tervek frissítése, a meglévőkön felül szükséges kiképzések és felkészítések végrehajtása, valamint szükség esetén az éles feladatellátás hatékony megvalósítása.

A belső szabályozás tekintetében szükségesnek mutatkozik még egy átfogó felülvizsgálat végrehajtása és szükség szerint új miniszteri utasítások kidolgozása az ágazati feladatok koordinált tervezése és végrehajtása érdekében. E körben egyrészt indokolt a korábbi, már elavult utasítások hatályon kívül helyezése, másrészt olyan új és összehangolt szabályozás kialakítása, amely a Korm. határozat esetleges módosításához igazodóan egységes keretek szerint határozná meg az egyes ágazatokon belüli feladatokat, figyelemmel már az Alaptörvény 51/A. cikke szerinti terrorveszélyhelyzettel összefüggő egyes feladatokra.

A hatályos és aktuális szabályozási lépéseken túl, hosszú távon és rendszerszinten szemlélve a terrorizmus elleni fellépés szabályozási és szervezeti vonatkozásait, megvizsgálandónak látom *a terrorizmust elhárító szerv jogállásának, szabályozásának és szervezetének felülvizsgálatát*. E körben egyrészt azt tartom mérlegelendőnek, hogy a megfelelő kormányzati hatáskörmegosztás és a fokozott törvényességi felügyelet biztosítása mellett nem lehet-e hatékonyabbá tenni a fellépést akkor, ha szervezeti szinten centralizáljuk az operatív és a műveleti feladatellátást? Ezzel értelemszerűen a terrorelhárítás egy olyan új védelmi ágazattá lépne elő,¹⁸ amely félúton helyezkedik el a rendészet és a nemzetbiztonság között, így kormányzati oldalról felvehető akár annak önálló belügyminisztériumi államtitkár általi felügyelete is, másrészt pedig egyértelműen szükségesnek mutatkozna ennek a különállásnak a törvényi megalapozása is.

Ez természetesen nem jelenti azt, hogy a terrorizmus elleni fellépés feladatai egyetlen szervnél összpontosulnának, hiszen úgy a közreműködő szervek, mint az egyes titkosszolgálatok tekintetében továbbra is kell ilyen feladatoknak szerepelnie. Ez a gondolat inkább abba az irányba mutatna, hogy némileg átláthatóbbá tegye a szabályozást és a szervezeti vonatkozásokat is ebben a témakörben, feltételezve, hogy a racionalizációval egybekötött feladat-centralizálás eredménye a hatékonyabb és gyorsabb feladatellátás, ami a fokozódó és kiszámíthatatlan terrorfenyegetettség tekintetében alapvető igény. Ennek lényegében a legtöbb feltétele – figyelembe véve

¹⁸ A fegyveres védelem rendszeréről és annak ágazatiról lásd: Farkas Ádám: Adalékok az állam fegyveres védelmének rendszertani megközelítéséhez. In Honvédségi Szemle 2017/1. szám, pp. 44-58.

a vonatkozó szabályozást – jelenleg már a személyi állomány összetétele, a feladatrendszer, a titkos információgyűjtés és a külföldön történő feladatellátás biztosítottága folytán egyaránt szabályozott.

Ezt a rendészeti és nemzetbiztonsági szféra közt létesülő új védelmi ágazati szisztémát a terrorelhárításon túlmutatóan tovább erősítené meglátásom szerint az is, hogy a kibertérben elkövetett cselekmények elleni fellépést jól látható időtávon belül mindenképp meg kell erősíteni úgy szervezeti, mint szabályozási szempontból. Ennek eszközrendszerét, lehetséges jogköreit, valamint költségigényét és ezzel összefüggésben átláthatóságának biztosítását számba véve tehát jó eséllyel a kibervédelem terén is megfontolható lenne egy ilyen köztes intézmény kialakítása. Ez a „csúcsszerv” a feladatok centralizált ellátása mellett egyúttal felelne az összes ágazat kibervédelmi tevékenységének koordinációjáért is és a hosszú távú stratégiák kialakításáért, úgy ahogy lényegében a Terrorellenes Koordinációs Bizottság vezetése révén a TEK főigazgatója is rendelkezik ilyen koordinációs feladattal már most is a terrorizmus elleni fellépés vonatkozásában. A kibervédelem ez irányú megjelenítés azért is aktuális e sorok között, mert a kiberterrorizmus fokozódása sem zárható ki a közeli jövőben, amely meglátásom szerint a terrorizmusról alkotott fogalmaink újragondolását épp úgy indokolni fogja, mint a szervezeti és intézkedési keretek fejlesztését, revízióját.

A hatályos szabályozás módosítására távlatosan irányuló javaslatok köréből zárásként még *a katonai értelemben vett terrorellenes műveleteknek, valamint a bukott államok vonatkozásában végzett béketeremtő és békefenntartó missziók hozadékainak az összekapcsolását vetném fel a tömeges bevándorlás okozta válsághelyzet kezelésével és a honi területen végzett terrorellenes tevékenységekkel.* E körben egyrészt felmerülhet az érintett szervek közti közreműködési szabályok felülvizsgálata és kétirányú fejlesztése:

1. Az esetleges azonosított terror-kapcsolatok esetén közös rendőri-katonai-nemzetbiztonsági műveletek végrehajtása a szövetségi keretrendszerekben végzett művelési felajánlások fejlesztésével, vagy időszakos kiegészítésével.
2. A hadművelési keretekben szerzett – leginkább különleges művelési – tapasztalatok transzformálása a hazai terrorizmussal összefüggő válságkezelésre, illetve közös rendőri-katonai műveletek végrehajtására történő felkészülésbe.

Másrésztől megvizsgálandó az információk megosztására vonatkozó protokollok erősítést célzó felülvizsgálatának lehetősége és a Magyar Honvédség szövetségi kapcsolatainak terrorellenes információkra vonatkozó kiaknázásának áttekintése is, különös tekintettel az ez irányú nemzetközi műveletek során szerezhető információkra, de akár a szövetségi keretben zajló továbbképzések tapasztalatainak honi terrorelhárításban történő felhasználására is.¹⁹

Harmadrésztől megvizsgálandó egy az Amerikai Egyesült Államok gyakorlatában már működő biometrikus adatrögzítési gyakorlat kialakítása,²⁰ amely

¹⁹ E körben jelentős fókuszpont lehet például a Törökországban települő NATO Centre of Excellence Defence Against Terrorism képzési, kutatási tevékenységében való részvétel erősítése és az ott szerezhető információk ágazatközi megosztása, kiaknázása.

²⁰ A téma visszhangja kapcsán lásd: WIRED: U.S. Holds on to Biometrics Database of 3 Million Iraqis. <https://www.wired.com/2011/12/iraq-biometrics-database/> (Letöltés ideje: 2017. 05. 25.), Public Intelligence: Identity Dominance: The U.S. Military's Biometric

a műveleti területen és a migrációs válság kezelése körében támadó- vagy terroristagyanúsnak minősített személyek begyűjtött adatait hozzáférhetővé tenné a vonatkozó megjelöléssel a hazai terrorelhárítók számára. Ez nyilván felveti a vonatkozó adatkezelési és büntügyi együttműködési szabályozás vizsgálatát és szükség szerinti módosítását épp úgy, mint a katonai erők ezen szabályozási körbe történő bevonását, azonban hosszabb távon a megfelelő törvényességi felügyelet mellett jelentős eszközt biztosíthat a hatékony megelőzés és elhárítás tekintetében, amennyiben tartják magukat azok a nemzetbiztonsági és biztonságpolitikai prognózisok, hogy a bukott államok, a migráció és a terrorizmus közti összefüggés jól kimutatható.²¹

Természetesen ezeken túlmenően több, átfogó személetű, hosszú távú fejlesztési javaslat is mérlegelhető úgy a szabályozás, mint az intézményi keretek tekintetében, ezeket azonban célszerű lenne önálló tanulmányokban, elemzésekben, koncepciókban megvizsgálni, majd mindezen felvetéseket egymással szinkronizálni.

3. Összegzés

A terrorizmus elleni fellépés szervezeti és szabályozási vonatkozásai tekintetében összességében az állapítható meg, hogy Magyarországon is egy több évtizedes változási, fejlődési folyamat valósult meg ezen témakör kapcsán, amely több lépcsőben és több síkon törekedett arra, hogy erősítse a terrorizmus elleni fellépéshez rendelkezésre álló szervezeti, képességbeli és jogi eszközöket.

Ez a fejlődési folyamat mindenképp üdvözlendő és különösen a 2015-től kezdődő jogalkotással új lendületet nyert az államszervezet és a reagálás intézményi skálája tekintetében, azonban még nem tekinthető lezártnak, vagy bevégeztnak. A terrorizmus elleni fellépés ugyanis jellegéből adódóan számos ágazatközi jellemzővel bír, ami meglátásom szerint a szabályozás és az intézményrendszer tekintetében is szükségessé tesz további korrekciókat és fejlesztéseket.

A szükséges módosításokat, fejlesztéseket két csoportra oszthatjuk a megvalósítás időtartama tekintetében. E körben a rövid távú fejleszthetőséget részint a meglévő szabályozási környezet pontosításában, részint pedig az erre épülő alacsonyabb szintű, közjogi szervezetszabályozói jellegű kiegészítésében és ezzel a felkészülés határfokának javíthatóságában látom.

A hosszú távú fejleszthetőség már több kérdést is felvet. E körben különösen a következők jeleníthetők meg:

1. A különleges jogrendre vonatkozó szabályozási tradíciók felülvizsgálata, valamint tágabb körben a fegyveres védelem szabályozásának rendszerszintű hazai revíziója a nemzeti sajátosságok, a nemzetközi minták, valamint a várható biztonsági változások figyelembevételével.

War in Afghanistan. <https://publicintelligence.net/identity-dominance/> (Letöltés ideje: 2017. 05. 25.)

²¹ A téma vonatkozásában érdemes megvizsgálni az újabb trendprognózisokat. E körben lásd: EUROPOL: European Union Terrorism Situation and Trend Report. Hague, European Union Agency for Law Enforcement Cooperation, 2017.

2. A terrorizmust elhárító szerv jogállásának, szervezetének, feladatrendszerének és ágazati hovatartozásának fejlesztés-orientált felülvizsgálata és a kibervédelem kérdésének párhuzamos vizsgálatával egy, a rendészet és a nemzetbiztonság közti új fegyveres védelmi ágazat kialakításának mérlegelése annak szabályozási és kormányzati vonatkozásaival egyetemben.

3. A terrorizmus elleni fellépés katonai hozadékainak összefűzése a hazai területen végzett terrorelhárítási tevékenységgel és ezáltal a rendőri-katonai-nemzetbiztonsági együttműködés erősítése ezen a téren.

Mindezek természetesen további vizsgálatokat, elemzéseket, majd koncepcionális javaslatok előkészítését teszik szükségessé, amelyben a kellő tudományos és szakmai alapok mellett egyértelműen szükséges a tudományos eredmények és javaslatok becsatornázása a központi közigazgatásba, majd ezek megmértése az ágazati és a kormányzati igényekkel, szándékokkal. Az azonban jelentősebb rizikó nélkül állítható, hogy a terrorizmus jelentette kihívás a jövőben is neuralgikus kérdése lehet az állam fegyveres védelmének és az ehhez kapcsolódó szervezetalakításnak, szervezetfejlesztésnek és szabályozásnak is. Erre figyelemmel a lehetséges fejlesztési irányok feltérképezése és az ezzel kapcsolatos diskurzus serkentése kiemelt jelentőségű lehet úgy a védelmi fejlesztések, mint az államreform és a közszolgálat-fejlesztés tekintetében, nem beszélve a rendőri-katonai-nemzetbiztonsági együttműködés fejlesztéséről.

Felhasznált irodalom:

- ARANY Anett – N. RÓZSA Erzsébet – SZALAI Máté: Az Iszlám Állam – következmények. Budapest, Külügyi és Külgazdasági Intézet KKI-tanulmányok T-2015/1, 2015.
- BARTKÓ Róbert: A terrorizmus elleni küzdelem kriminálpolitikai kérdései. Győr, Universitas-Győr Nonprofit Kft., 2011.
- BEKE József – DR. HEGYES Gabriella: A terrorelhárítás kezdetei Magyarországon - A C-79-es dosszié. In (T)Error & elhárítás 2015/I. szám. http://tek.gov.hu/tt_pdf/2015/bekedrhegyes.pdf (Letöltés ideje: 2017. 05. 25.)
- BESENYŐ János – PRANTNER Zoltán – SPIEDL Bianka – VOGEL Dávid: Iszlám Állam. Terrorizmus 2.0. Történet, ideológia, propaganda. Budapest, Honvéd Vezérkar Tudományos Kutatóhely – Kossuth kiadó, 2016.
- Charles TOWNSHEND: Terrorizmus. Budapest, Magyar Világ Kiadó, 2003.
- EGENDORF Laura K. (ed.): Terrorism: opposing viewpoints. San Diego, Greenhaven Press, 2004.
- Ekaterina STEPANOVA: Terrorism in asymmetrical conflict. Ideological and Structural Aspects. Oxford, Oxford University Press, 2008.
- EUROPOL: European Union Terrorism Situation and Trend Report. Hague, European Union Agency for Law Enforcement Cooperation, 2017.

- FARKAS Ádám: Adalékok az állam fegyveres védelmének rendszertani megközelítéséhez. In Honvédségi Szemle 2017/1. szám, pp. 44-58.
- FARKAS Ádám: Gondolatok a terrorveszélyhelyzetről. In Szakmai Szemle 2016/3. szám, pp. 174-189.
- FARKAS Ádám: Szemléletváltást védelmi aspektusban! In Pázmány Law Working Papers 2015/18. szám.
http://d18wh0wf8v71m4.cloudfront.net/docs/wp/2015/2015-18_Farkas_.pdf
(Letöltés ideje: 2017. 05. 25.).
- FARKAS Ádám: Tévelygések fogságában? Tanulmányok az állam fegyveres védelmének egyes jogtani és államtani kérdéseiről, különös tekintettel Magyarország katonai védelmére. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2016.
- HAVASI Zoltán: A terrorizmus és a jog. In Nemzetvédelmi Egyetemi Közlemények 2003/4. szám pp. 46-68.
- HEGEDŰS Ernő: Terrorelhárító erők szervezése a rendvédelmi szervezeteknél és a légi deszant csapatoknál. In Rendvédelem-történeti füzetek 2010/22. szám, pp. 53-59.
- Jonathan BARKER: A terrorizmus. Budapest, HVG kiadó, 2003.
- Kenneth KATZMAN – Christopher M. BLANCHARD – Clara E. HUMUD – Rhoda MARGESSON – Matthew C. WEED: The „Islamic State” Crisis and U.S. Policy. Washington, Congressional Research Service, 2015.
- KESZELY László: A NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer alkalmazásának tapasztalatai az ukrán válsággal összefüggésben. In Hadtudomány 2015/1-2. szám, pp. 120-125.
- KESZELY László: A NATO válságreagálási rendszerével összhangban álló nemzeti intézkedési rendszer és a különleges jogrend összefüggései. In Katonai jogi és hadijogi szemle, 2014/1. szám, pp. 191-221.
- KIS-BENEDEK József: Az Iszlám Kalifátus és a globális dzsihád új tendenciái. In Hadtudomány 2014/3-4. szám, pp. 22-33.
- KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus. Budapest, Zrínyi kiadó, 2016.
- Loretta NAPOLEONI: Az iszlamista főnix, Az Iszlám Állam születése és a Közel-Kelet újrafelosztása. Budapest, HVG kiadó, 2015.
- Marie-Helen MARAS: A terrorizmus elmélete és gyakorlata. Budapest, Antall József Tudásközpont, 2016.
- Michael WEISS – Hassan HASSAN: Az Iszlám Állam. A terror hadserege belülről. Budapest, HVG kiadó, 2015.
- N. RÓZSA Erzsébet: Az Iszlám Állam előretörése Irakban és az amerikai válaszcsepások. In Nemzet és Biztonság 2014/4. szám, pp. 56-61.
- PÓCZIK Szilveszter: A terrorizmus kriminológiai perspektívában. In Rendészeti Szemle. 2006/9. szám pp. 45-59.

- PÓCZIK Szilveszter: Bevezetés a terrorizmus kriminológiájába I. rész. Definíció, tipológia, jog és történelem. In Irk Ferenc (szerk.): Kriminológiai Tanulmányok 43. Budapest, Országos Kriminológiai Intézet, 2006, pp. 63-94.
- Public Intelligence: Identity Dominance: The U.S. Military's Biometric War in Afghanistan. <https://publicintelligence.net/identity-dominance/> (Letöltve: 2017. 05. 25.)
- RESPERGER István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői. In Hadtudomány 2010/4. szám, pp. 68-77.
- SELJÁN Péter: Harc az Iszlám Állam ellen. In Nemzet és Biztonság 2014/5. szám, pp. 63-74.
- SIMICSKÓ István: A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével. In Hadtudomány 2016/3-4. szám, pp. 100-113.
- STEWART Gail B.: Terrorism. San Diego, Kidhaven Press, 2002.
- TÁLAS Péter (szerk.): A terrorizmus anatómiája. Budapest, Zrínyi Kiadó, 2006.
- TAYLOR Robert: History of Terrorism. San Diego, Lucent Books, 2002.
- WIRED: U.S. Holds on to Biometrics Database of 3 Million Iraqis. <https://www.wired.com/2011/12/iraq-biometrics-database/> (Letöltve: 2017. 05. 25.)

Felhasznált jogforrások:

- A rendőrségről szóló 1994. évi XXXIV. törvény.
- A Magyar Népköztársaság belügyminiszterének 26/1979. számú parancsa a BM III. (Állambiztonsági) Főcsoportfőnökség Ügyrendjének kiadásáról.
- A terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény rendelkezéseit.
- A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény.
- A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény.
- A terrorizmus elleni küzdelemről, a pénzmosás megakadályozásáról szóló rendelkezések szigorításáról, valamint az egyes korlátozó intézkedések elrendeléséről szóló 2001. évi LXXXIII. törvény.
- A robbantásos terrorizmus visszaszorításáról, New Yorkban, az Egyesült Nemzetek Közgyűlésének 52. ülészakán, 1997. december 15-én elfogadott nemzetközi egyezmény kihirdetéséről szóló 2002. évi XXV. törvény.
- A terrorizmus finanszírozásának visszaszorításáról, New Yorkban, az Egyesült Nemzetek Közgyűlésének 54. ülészakán, 1999. december 9-én elfogadott nemzetközi egyezmény kihirdetéséről szóló 2002. évi LIX. törvény.
- A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2007. évi CXXXVI. törvény.

- Az Európa Tanács terrorizmus megelőzéséről szóló, Varsóban, 2005. május 16-án kelt Egyezménye kihirdetéséről szóló 2011. évi II. törvény.
- A NATO Válságreakálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről szóló 278/2011. (XII. 20.) Korm. rendelet.
- A NATO Válságreakálási Rendszerrel összhangban álló Nemzeti Intézkedési Rendszer működtetésével kapcsolatos feladatokról szóló 20/2014. (III. 21.) HM utasítás.
- A Magyar Honvédség által védendő létesítmények kijelöléséről, valamint a magyar állam folytonosságát és függetlenségét megtestesítő ereklyék köréről és az őrzésükre vonatkozó szabályokról szóló 78/2011. (V. 12.) Korm. rendelet.

Bevezetés

A korrupció, a gazdasági kudarcok és az ukrán társadalmi igazságtalanságok ellen küzdő és a nyugati integrációt zászlajára tűző mozgalom, a 2013-14-es Euromaidan kijeji összecsapásaival Ukrajna és a hadtudomány életében is új korszak kezdődött. A forradalom, majd Viktor Janukovics elnök elűzése – és az orosz különleges erők által Oroszországi Föderációba (továbbiakban: Oroszország) menekítése – után először fegyveres összetűzésekké átalakult, majd nemzetközi konfliktussá eszkalálódó ukrán konfliktus – hírértékét veszítve, a világ- és közmédiában kevésbé megjelenítve – napjainkban is tart. Hosszú távú, változó intenzitású konfliktus, amely nemcsak Ukrajna határait rajzolta át, de az orosz–NATO–EU–USA kapcsolatokat is alapjaiban változtatta meg. Ukrajna nyugatbarát ellenzéke, amellyel szemben állt Kelet-Ukrajna oroszbarát, vagy eredendően orosz etnikumú kisebbséggel, kérlelhetetlen és eddig feloldhatatlan feszültséget szült. Vlagyimir Putyin az Oroszország érdekeit eredendően sértő NATO és EU felé orientálódó új Ukrajnával szemben egyre nyíltabban támogatta a mind markánsabbá váló donyecki és luhanszki szeparatista törekvéseket. Ez a folyamat vezetett később a fegyveres agresszióhoz.

Oroszország kezdetektől fogva reguláris, irreguláris és félkatonai egységekkel, továbbá különleges műveleti csoportokkal, titkosszolgálati eszközökkel, hírszerzési információkkal és jelentős légvédelmi, tüzérségi, és páncélos nehézfegyverzettel támogatta a magukat felkelőknek hirdető fegyvereseket. Ennek nyilatkozott indoka a humanitárius segítségnyújtása volt.¹ Az orosz külpolitika legitimálni törekedett a Luhanszki és a Donyecki Népköztársaságokat. A cél elérése érdekében politikai eszközökkel közvetlen és közvetett nyomást gyakorolt Ukrajnára és Európára is. Oroszország a háttérből irányítja a szakadókat és képviseli őket a tárgyalásokon, a tüzszüneti tárgyalásokon, illetve a minszki megállapodásoknál.² Az orosz fél delegált tanácsadóin és orosz államvédelmi múlttal rendelkező szakadár vezetőikön keresztül tevékenyen részt vett a kiszakított területek állami szervezeteinek megszervezésében, még ha ezt Oroszország többször is tagadta. A 2014-ben nyíltá vált orosz-ukrán szembenállás, és a konfliktus egyik kezdeti csúcspontja a szevasztopoli haditengerészeti bázis orosz ellenőrzés alá vonása, illetve a Krím-félsziget Oroszország általi annektálása volt. A Krím-félsziget megszállása során a csekély ellenállást tanúsító ukrán haderő lefegyverzése, majd a katonai kényszerrel

¹ Unian.info: Humanitarian intervention as basis for using force against another nation, <https://www.unian.info/world/1104120-humanitarian-intervention-as-basis-for-using-force-against-another-nation.html> (Letöltés ideje: 2017. 09. 17.)

² DEARDEN, Lizzie: Vladimir Putin issues executive order recognising documents issued by separatists 'republics' in Ukraine, <http://www.independent.co.uk/news/world/europe/vladimir-putin-donald-trump-ukraine-war-crimea-rebels-separatists-executive-order-documents-donetsk-a7587666.html> (Letöltés ideje: 2017. 09. 17.)

manipulált népszavazás Ukrajna szuverenitásának súlyos megsértését jelentette.³ Az agresszív oroszországi terjeszkedés egyértelmű felelőmet keltett Kelet-Európában és a Balti államokban.

A robbanáspontra Oroszország és az EU országainak kétoldalú kapcsolatai is mélypontra kerültek, felfüggesztették a katonai, a gazdasági, a politikai együttműködéseket. Az USA és az EU embargóval, illetve gazdasági szankciók egész sorával sújtotta az Oroszországot, amelyhez más fejlett államok (pl.: Kanada és Japán) is csatlakozott. Oroszország válaszul az érintettekkel szemben egyes importcikkekre jelentett be korlátozásokat.

Miben volt más az orosz konfliktus, mint a korábbi, az európai kontinensen lezajlott konfliktusok? Az orosz-ukrán konfliktus megmutatta Európának és a világnak az állami vezetés teljeskörű támogatásával aprólékosan megtervezett és gyorsan kivitelezett aszimmetrikus hadviselés destabilizáló erejét.

A konfliktus kezdete⁴

Az eddigi kutatásaim szerint a hálózat alapú hadviselés⁵, a diverziós csoportok rekord gyorsasággal zilálták szét az ukrán erők közötti kommunikációt, rombolták a kritikus infrastruktúrát, és vették át az irányítást a kérdéses területen. Kulcsmomentumként sikeres harctevékenységet végeztek az ukrán forradalomként jellemzett események után⁶ részben demoralizált és szétesett, de mégis a viszonylagos szervezeti egységét megőrző és teljes felszereltségével rendelkező ukrán haderő ellen. Az ukrán hálózatok nem voltak védettek, ezért az energia és a távközlési hálózatokat könnyen szét lehetett zúzni a kiberhadviselés eszközeivel is.⁷ Ez a sors várt a többi puha célponton, elsősorban az államhatalmat képviselő hivatalokra, a speciális különítmények révén pedig az ukrán SZBU⁸ épületeire. A donyecki területek elvesztése ráadásul negatívan befolyásolta Ukrajna energetikai ellátását, ipari központ lévén. Az információs környezetben folytatott műveletek⁹ a kritikus kezdeti időszakban (Krím, Kelet-Ukrajnába történő orosz betörés) hatékonyan demoralizálták az ukrán csapatokat, zavarták össze az ukrán belpolitikát

³ OSCE (EBESZ): Minsk Declaration, <https://www.oscepa.org/documents/all-documents/annual-sessions/2017-minsk/declaration-25/3555-declaration-minsk-eng/file> (Letöltés ideje 2017. 09. 17.)

⁴ A tanulmány szerzőjeként elsősorban nem katonai szakértőként vizsgáltam a konfliktus katonai jellemzőit, hanem a korábbi biztonságpolitikai tanulmányaimra, és az egyes alkalmazott fegyverek iránti technikai érdeklődésemre támaszkodva. Kutatásaimat a konfliktus kapcsán íródott és fotózott internetes tartalmak inspirálták. Bővebben: SZENTIRMAI Péter: Az ukrán válság katonai oldalának új kihívásai OTDK, Budapest 2017.

⁵ RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés – Kis háborúk nagy hatással, Zrínyi Kiadó, 2014.

⁶ Híradó.hu: Három éve ért véget Ukrajnában a forradalom <https://www.hirado.hu/2017/02/22/harom-eve-ert-veget-ukrajnaban-a-forradalom/?source=hirkereso> (Letöltés ideje: 2017. 09. 17.)

⁷ Bővebben: HAIG Zsolt: Információ Társadalom Biztonság, NKE Szolgáltató Kft., 2015.

⁸ Ukrajna egyik nemzetbiztonsági szolgálata, az Ukrán Biztonsági Szolgálat (ukránul: Служба безпеки України – rövidítve: SZBU)

⁹ SIMON László: Az információ, mint fegyver? KNBSZ Szakmai Szemle 2016. 1. szám, http://www.knbsz.gov.hu/hu/letoltes/szsz/2016_1_szam.pdf (Letöltés ideje: 2017. 10. 15.)

és manipulálták a nemzetközi közvéleményt, valamint rajtuk keresztül a kormányzati állásfoglalást.

A pszeudo és reguláris¹⁰ erők mindkét oldalon jelentős szerepet játszottak a haderőn belül. A hadifoglyok, civilek, harcoló katonák körében hamar hírhedté váltak az orosz különleges műveleti múlttal rendelkező Igor Bezler, és Givi nevű katonai vezetők rendkívül heves és eredményes harcai, illetve az általuk elkövetett atrocitások. A félkatonai szervezetek állományának ellenőrizhetetlen múltja, a kezükbe kerülő fegyverzet nemcsak regionálisan, de Ukrajna más térségeiben is problematikus. Az ukrán szélsőjobbaldali milíciák Kárpátalján fegyveres összetűzésbe kerültek például Mihajlo Lanyo ellenzéki politikus testőrségével¹¹, illetve a rendőrséggel is, és fegyverzetüket nem adják le, kvázi függetlenül magukat az ukrán fegyveres erők szervezetével, sokszor önállóan tevékenykedve. Külön hátránosnak tartom, hogy a legmodernebb T-64BM Bulat harckocsik közül is több darabot kapott az Azov-zászlóalj.¹² Ennek ellenére a harctevékenység során többször cserbenhagyták a hadsereget, haderejükkel többször az ukrán államigazgatást sakkban tartva.

A konfliktus társadalmi vetületében ideológiai, vallási és kulturális jellemzők is jelen voltak. Ideológiailag szembe kerültek a nyugati demokratikus, illetve a keleti tekintélyelvű, korlátozott elnöki demokrácia(?) hívei. Ez éles választóvonalaként különült el a keleti és a nyugati területek között. A kulturális és a vallási feszültség a nyugati katolikus és a keleti ortodox vallási irányzatok között figyelhető meg. Utóbbi egyértelműen az orosz kultúrkör befolyása, és az orosz ambíciók egy kivetülése. Az orosz ortodox egyház a Szovjetunió összeomlása óta a diaszpórában, illetve kisebbségben élő orosz népcsoportok számára egyértelműen kulturális jelzőfény, az identitástudatuk őrzője, egyúttal az orosz politika szoros szövetségese a regionális nyomásgyakorlás terén, felhasználva a kisebbségi ütőkártyát a Baltikumban. Ezen csoportok mobilizációs képessége magas, ezt figyelhettük meg Ukrajna esetében is. A média által végrehajtott kommunikáció, sőt inkább dezinformáció segítette a szakadár fegyveres erők nagyszámú utánpótlását. Az „elme háborúja”, a tömegek feletti kontroll és irányítás mindvégig az orosz félnek kedvezett. A dezinformációs csatornák bomlasztották az ukrán háttérország egységét.¹³ Ez a fenyegetés az „EU-ba vetett bizalomra” annyira kényes volt, hogy 2015-ben létrehozták az East Stratcom Task Force-ot, amelynek elsődleges feladata az orosz

¹⁰ KEMÉNY János: A felkelésellenes hadviselés lakosságközpontú elméletének fejlődése a XX-XXI. században, http://phd.lib.uni-corvinus.hu/769/1/Kemeny_Janos.pdf (Letöltés ideje: 2017. 10. 15.)

¹¹ TiszaNews.org.ua: Több mint 10 fegyveres rejtőzködik Munkácsnál, <http://tiszanews.org.ua/?module=news&&target=get&id=8774> (Letöltés ideje: 2017. 09. 17.)

¹² Az AZOV-zászlóalj később AZOV hadtest ukrán milícia, Bővebben: <http://www.dailymail.co.uk/news/article-3195711/Now-CHILDREN-taking-arms-Shocking-pictures-inside-Ukraine-s-neo-Nazi-military-camp-recruits-young-six-learn-fire-weapons-s-ceasefire.html> (Letöltés ideje: 2017. 10. 15.)

¹³ Euromaidan Press: Ukraine targeted by disinformation campaign to restore "friendship" with Russia, <http://euromaidanpress.com/2017/01/12/fake-news-campaign-in-ukraine-presses-to-restore-economic-relations-with-russia/#arvlbdata> (Letöltés ideje: 2017. 09. 17.)

dezinformációs műveletek monitorozása, és tevékenységük lakosságra gyakorolt hatásának neutralizálása.¹⁴

Az itt felsorolt elemek mind a hibrid műveletek első újszerű, európai megvalósításának kulcselemei. Véleményem szerint, dacára a NATO csapatok iraki és afganisztáni tapasztalatainak, modern harceljárásainak, az orosz módszer alapjaiban veszélyes a modern infokommunikációs¹⁵ Európa fejlett társadalmaira, a többfajta, alapvetően koherens rendszerek szimbiózisszerű működésére. Itt gondoljunk csak a 2007-es észtországi katonai jellegű hekkertámadásra. Az eseményeket az európai politikai vezetés a konfliktus kiszélesedésének időszakában benuhátsággal fogadta. A katonai vezetés sem rendelkezett hasznos megoldásokkal, amellyel eredményesen támogathatták volna az ukrán erők felkelésellenes műveletét. Kiemelten fontosnak tartom régiónk szempontjából a szomszédos országokra áttevődő veszélyeztetést és a destabilizálódó állam negatív jelenségeit, amely a szervezett bűnözés növekedése, fegyverkereskedelem, politikai szélsőségek és hadviselt személyek beszivárgó tevékenységében és a gerjesztő mag-állam mind nagyobb külpolitikai nyomásában erősödhet fel. Európának a gyakorlatban fel kell készülnie az aszimmetrikus kihívásokra, amely akár Oroszország, akár más nagyhatalom érdekszférájában elhelyezkedő országban hasonló forgatókönyv szerint bármikor bekövetkezhet.

A konfliktus politikai és jogelméleti háttere

Ukrajna alapvetően az európai, nyugati civilizáció keleti határán fekszik, kijáráttal az Azovi- és a Fekete-tengerre. Kikötői: Mariupol, Odessza, Szevasztopol, Mikolajev katonai és kereskedelmi szempontból is kiemelt fontosságúak. Energetikai csomópont, több földgáz- és kőolajvezeték is keresztülhalad területén, többek között a hazánkba tartó Barátság-I-II.¹⁶ Ha kitekintünk, láthatjuk, hogy a Szovjetunió összeomlása után hagyományosan ismét két hatalmi tömb malomkövei között őrlődik: az Egyesült Államok támogatta Európai Unió, illetve az Oroszország közötti ütközőzónaként. A nyugatbarát és oroszbarát kormányok váltakozása állandó külföldi nyomásgyakorlásnak tette ki az országot. Ennek legemlékezetesebb példája a 2009-es orosz-ukrán gázvita¹⁷, amely Magyarországon is komoly földgázhiányt okozott, Szerbiában pedig energetikai krízist. Moszkvát pedig alapvetően sértette a 2008-ban megkezdődött EU–Ukrán szabadkereskedelmi társulási tárgyalás, amely döntően a nyugat karjaiba sodorhatja az országot. Ukrajna politikai instabilitására és

¹⁴ EEAS: Questions and Answers about the East StratCom Task Force, http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2015/261115_stratcom-east_qanda_en.htm (Letöltés ideje: 2017. 10. 15.)

¹⁵ BALOGH Fatime - FEKETE Csanád – NÉMETH András – NÉMETH József Lajos: A hibrid hadviselés különös tekintettel a mobil kommunikációra, http://www.hadmernok.hu/154_12_balogf_na_joe.pdf (Letöltés ideje: 2017. 10. 15.)

¹⁶ A Dnyeper, Donyeck és Azov ércében gazdag régiójára komplex vaskohászati ipar települt, amely a Dunai Vasművel is szoros együttműködésben áll. Vallásában a római katolikus és a görög-keleti ortodox között megosztott. Kulturálisan is vegyes képet mutat, ukrán, orosz, fehérorosz, moldáv, bolgár, tatár, szlovák, lengyel és magyar etnikum lakja.

¹⁷ VARGA Tamás: Az orosz-ukrán gázvita, http://kitekinto.hu/europa/2009/01/08/az_orosz-ukran_gazvita (Letöltés ideje: 2017. 11. 08.)

antidemokratikus berendezkedésére jellemző lehet például az oroszbarát nyomásra letartóztatott Julija Tyimosenko nyugatbarát ellenzéki vezető.¹⁸

Ennek a nyomásnak volt a csúcspontja a 2013. november 21-én ukrán részről felfüggesztett társulási megállapodás. Még ezen a napon tüntetések kezdődnek Kijevben, a Majdan Nezalezsnosztyi (Függetlenség) téren. Decemberre elmérgesedik a helyzet, itt csapnak össze először a nyugatbarát-jobboldali erők és a Janukovicshoz hű erők. Az összecsapások során több mint 100 embert öltek meg a felfegyverkezett civilek közül. A forradalom győzelme után az egységet feloszlatták, tagjai közül sokan dezertáltak és a Krímbe, illetve Kelet-Ukrajna szakadár ellenőrzésű területeire menekültek folytatni a harcot.¹⁹ (A harcok végül 2014. január 28-án az ukrán kormány lemondásához vezetnek, majd februárban Janukovics elnök Oroszországba „szökött”.)

A Krím-félsziget leválasztása február 27-én vette kezdetét, amikor akkor még ismeretlen fegyveresek foglalták el a főbb csomópontokat, útvonalakat, kormányhivatalokat. 2014. március 1-jén az orosz beavatkozási szándékot hivatalos lehetőségként formába öntve a Duma jóváhagyta a fegyveres erő alkalmazását Ukrajna területén (nyílt beavatkozásra nem került sor). Az ukrán kormány a politikai és katonai vezetés dezorganizáltsága miatt nem tudta megfelelően kezelni a helyzetet és egységesen fellépve megakadályozni a szeparatista tevékenységet. A Krímbe vitatható népszavazást tartottak 2014. március 16-án, amelyben 97%-os többséggel megszavazzák az Ukrajnától való elszakadást. A választás egyértelműen csalás volt, az ellenőrzésre a helyszínre érkező EBESZ-t képviselő személyekre a fegyveresek rálóttek, az ukránbarát krími lakosságot és a krími tatár kisebbséget megfélemlítették, sokszor fizikailag is bántalmazták, nem engedték leadni az Ukrajna-párti voksokat. Egy nappal később Putyin elnök elismerte Krím függetlenségét, majd törvényjavaslatban jóváhagyták az Oroszországhoz való csatlakozást köztársasági státuszban. Április 7-én orosz háttértámogatással vette kezdetét Luhanszk és Donyeck lázadása a kijevi központi hatalom ellen. Az EU a politikai közléseken túl ismét csak gazdasági segítséget nyújtott. Az Ukrajnából érkező áruk vámjának 98%-os csökkentését iktatták be. Május 11-én a krími politikai forgatókönyv játszódott le Kelet-Ukrajnában is azzal a különbséggel, hogy Oroszország nem annektálta az Ukrajnából kivált két tartományt. (A nyugati országok természetesen nem ismerik el a mai napig sem a függetlenséget.) 2014. június 27-én az új ukrán elnök, Petro Porosenko aláírta az EU-Ukrajna társulási megállapodást, valamint a nyár folyamán az EU gazdasági szankciókat vezetett be Oroszországgal szemben. Ennek kapcsán hosszas hezitálás után, morális okokból, Franciaország nem szállított le két Mistral-osztályú helikopterhordozót. A szankciók 2015-re már 90 milliárd eurós veszteséget okoztak Oroszországnak, a külkereskedelme 30%-kal csökkent, ami a GDP 5%-os visszaesését okozta.

¹⁸ EP Hírek: Kronológia az ukránjai eseményekről,
<http://www.europarl.europa.eu/news/hu/news-room/20140203STO34645/kronol%C3%B3gia-az-ukrajnai-esem%C3%A9nyek%C5%911> (Letöltés ideje: 2016. 10. 16.)

¹⁹ BALMFORTH, Richard – Reuters: Ukraine’s new rulers disband riot police,
<http://www.reuters.com/article/us-ukraine-crisis-berkut-idUSBREA1P0AK20140226>
(Letöltés ideje: 2016. 10. 16.)

Az EU fokozta Ukrajna és a Porosenko-kormány politikai támogatását az EU–Ukrajna társulási szerződésének ratifikálásával szeptember 16-án. A megállapodáshoz tartozó szabadkereskedelmi zóna mélyítheti a gazdasági integrációt, és biztosíthatja a piacokhoz való kétoldalú hozzáférést.²⁰ A gazdasági mellett az USA katonai támogatást is nyújtott, 300 tanácsadó formájában. Ez az első eset a hidegháború óta, hogy amerikai katonai tanácsadók az orosz katonai alakulatok elleni harcra képeztek ki katonákat. A Pentagonban később döntöttek a Kelet-Európában rotációs rendszerben telepítendő mintegy 4500 fős páncélosdandár állomásoztatásáról, a szövetségesi bizalomerősítés és az orosz elrettentés céljából. (A NATO keleti szárnyának megerősítése céljából²¹ az észak-kelet-lengyelországi Orszyszba 2017. március 26-tól érkeztek a nemzetközi zászlóalj egységei.²²)

A kelet-ukrajnai felkelés kitörése

A „forradalom győzelme”²³ után szinte azonnal oroszpárti tüntetések kezdődtek Odessza, Mikolajiv, Herszon, Krím-félsziget, Zaporizzsja, Dnyipropetrovszk, Harkov, Donyeck és Luhanszk oblastok területén. A forradalom a politikai ellentétek, a korrupció, az elszegényedés, a munkanélküliség és az inkompetens kormányzás egyvelegének a következménye, addig láthatóan más lakosságot megmozgató ok a Donyeckben. Az orosz-ukrán konfliktus eszkalációját az állam domináns, etnikai és vallási, kulturális többségével szembehelyezkedő, erős

²⁰ EP Hírek: Az Európai Parlament ratifikálta az EU és Ukrajna közti társulási szerződést, <http://www.europarl.europa.eu/news/hu/news-room/20140915IPR62504/az-eur%C3%B3pai-parlament-ratifika%C3%A1lta-az-eu-%C3%A9s-ukrajna-k%C3%B6zti-szer%C3%A1si-szerz%C5%91d%C3%A9st> (Letöltés ideje: 2016. 10.16.)

²¹ Ukrajna jelentős nukleáris fegyverezését 1994-es budapesti memorandumban foglaltak szerint leszerelte. Ellentételezőként az aláíró hatalmak kötelezték magukat, hogy az ország területi integritását veszélyeztető esemény során ellenlépéseket tesznek. In: CFR.org: Budapest Memorandums on Security Assurances, 1994, <http://www.cfr.org/nonproliferation-arms-control-and-disarmament/budapest-memorandums-security-assurances-1994/p32484>. A memorandum szerint a Krím leválasztása és a szakadár területek fegyveres és politikai támogatása kimeríti a területi integritás veszélyeztetését, ugyanakkor az aláíró felek nem teljesítették vállalásaikat. Ukrajna, mint az orosz holdudvar nagyhatalmi érdekek szerint kiemelt figyelmet élvező területe, érzékeny pont: nagyhatalmi elköteleződés mellett komolyabb rakétafegyverzettel elérhető Oroszország teljes területe. A kérdést aktuális megvilágításba teszi a NATO rakétavédelmének tervezett kelet-európai kiterjesztése és az ukrán NATO-tagság távlati célja, mely az orosz álláspont szerint elsőszámú fenyegetés hazájukra nézve. In: NATO: Relations with Ukraine, http://www.nato.int/cps/en/natolive/topics_37750.htm, – Nato.mfa.gov.ua: NATO – Ukraine cooperation in the military sphere, <http://nato.mfa.gov.ua/en/ukraine-nato/military>, A NATO tagság a krími helyzet kapcsán, Ukrajna belpolitikai instabilitása, valamint a NATO tagállamok konfliktuskerülése a várható orosz ellenlépések miatt nem realizálódhat. In: VENDRICZKI Gábor – Ukrajna: NATO-tagság, vagy sem? – http://kitekinto.hu/europa/2015/10/19/ukrajna_nato-tagsag_vagy_sem (Letöltés ideje: 2016. 10. 25.)

²² MTI: Amerikai páncélos dandár jön Kelet-Európába, <http://www.hirado.hu/2016/03/30/amerika-egy-pancelos-dandart-telepit-kelet-europaba/> – MTI: Megérkezett Lengyelországba a NATO nemzetközi zászlóaljának első kontingense, http://www.nyugat.hu/tartalom/cikk/134932_megerkezett_lengyelorszagba_a_nato_nemzetkozi_elso (Letöltés ideje: 2017. 10. 15.)

²³ BBC News: Ukraine crisis: Timeline, <http://www.bbc.com/news/world-middle-east-26248275> (Letöltés ideje: 2017. 09. 17.)

identitású nacionalista–etnikai–szeparatista mozgalom fegyveres műveletei jelentették. A különálló identitás egyik meghatározó motívumaként erős, de nem fundamentalista vallási nemzetközi háttértámogatást élveztek. Az ortodox vallási jelképek rendszeresen megfigyelhetők voltak a szakadár egyenruhákon, harcjárműveken, amíg a templomok, mint kulturális, segélyező helyek egyfajta központként működtek, illetve az orosz politikai szemlélet exportcsatornájaként. A forradalom miatt működésképtelenné váló állami adminisztráció az élet alapvető területeire hatott ki, amely miatt az állampolgár más alternatívákat kezdett keresni, amely szintén katalizátora nemcsak a lázadásnak, hanem a korrupciónak és szervezett bűnözésnek is. Az államszervezeti káosz a rendvédelem hiányával párosulva hamar működésképtelenné tette a keleti területeket. A keleti oblastokba átcsoportosított, többségében ukrán identitástudatú katonai alakulatokat nemzetidegen csapatteknek tekintették az orosz etnikumú lakosok, ami sértette a nemzeti büszkeségüket. Így a tüntetések részben spontán, részben az orosz média, diplomácia által is feltűzelt és az FSB, GRU által támogatott tüntetések²⁴ hamar radikalizálódtak, és átsaptak utcai lázongásokba, barikádemelésbe, és az ukrán közszolgálati intézmények, és rendvédelmi erők létesítményei elleni támadásokba. Az államhatalmi célpontok elleni támadásokkal hamar aláásták a helyi ukrán erőkhöz vetett bizalmat. A megmozdulásokban részt vevő szeparatista civilek erős orosz identitástudatú nacionalista kötődésűek voltak.²⁵ Az aktivizált nagyszámú szeparatistával Oroszország kezdetől fogva megpróbálta alátámasztani az állítását, hogy az orosz kisebbséget a forradalom elnyomja. Véleményem szerint az ukrán vezetés elkövette azt a hibát, hogy a társadalmi felkelés politikai-gazdasági gyökerét nem tudták semlegesíteni. Hiányzott politikájukból a sikeres meggyőzés, amellyel jobb alternatívát kínáltak volna főleg szociális támogatással és gazdasági infrastrukturális fejlesztésekkel, mint amit az orosz politikai-katonai szembenállás jelentett nekik.

Nyomásgyakorlás a gazdaságra

Az ukrániai oroszok a gazdaság több kulcsfontosságú területét uraló vállalatban a nyugatbarát „bábkormány” idegen érdekeket kiszolgáló domináns szereplőit látták. A harcok kitörése után ezek a cégek célponttá váltak, kiváló támadási felületet kínálva politikai és média-szempontról. A modern aszimmetrikus műveletek fontos elemeként megjelent a gazdasági háttérbázis rombolása, illetve saját szolgálatba állítása. Ez szintén megvalósult az orosz vállalatok átgondolt krími és ukrániai expanziójával. A harcok kirobbanása után a szakadár ellenőrzésük alá vonták az ISD donyecki kohászati kombinátjait.²⁶ A harcok miatt munkanélkülivé vált bányászok tüntetéseikkel tovább gerjesztették a negatív spirált, amivel Oroszország igazolni tudta a nemzetközi és a belföldi propagandáját. A bányászok helyzetéhez hasonlóan alakult az oligarchák által szervezett footballhuligánok mozgósítása, a rendzavarás céljából történő gerjesztett

²⁴ BBC News: Ukraine crisis: Timeline, <http://www.bbc.com/news/world-middle-east-26248275> (Letöltés ideje: 2017. 09. 17.)

²⁵ NSDC of Ukraine: The Situation in the Eastern Regions of Ukraine, http://www.mbo.gov.ua/files/2014/RNBO_map_11_07_eng.jpg (Letöltés ideje: 2017. 11. 10.)

²⁶ ISD Dunaferr: Együtt a jövőbe, <http://www.dunaferr.hu/hu/> (Letöltés ideje: 2016. 12. 30.)

cselekmények, az Ahmetov-jelenség.²⁷ Az ukrán állami tulajdonú bányák kitermelése egyik következményként 48-70%-kal zuhant 2015-re.²⁸

A civilekre gyakorolt hatás

A konfliktus során a civilek végig a frontvonalban voltak, különösen igaz ez Luhanszk és Donyeck megyékre, ahol jelentős harccselekmények folytak. A civileket mindkét fél részéről érték negatív behatások. Ezeket az eseményeket a felkelők propagandája kíméletlenül ki is használta, sőt az orosz oldal ezt még igyekezett növelni is a civilek visszatartásával, a menekülésük akadályozásával. A városok belterületein állomásozó nehézfegyverzet nyilvánvalóvá teszi a „civil pajzs” kényszeredett jelenlétét. A felek által gerjesztett félelemfaktor is eltérő volt. Az ukrán erőket kötötte a nemzetközi hadijog, a civilekkel szemben alkalmazott intézkedéseik, a területek elfoglalása utáni „patkányirtó” műveletek szabályozott keretek között zajlottak. Tekintéllyel rendelkeztek a lakosság körében, ugyanakkor elrettentő erőt sokszor nem mutattak, ez utóbbi inkább csak a szélsőjobboldali milíciákra volt jellemző, a túlkapások zömével együtt. Ezzel szemben az oroszokat támogató felkelő, irreguláris csapatok sokrétű háttérük (civil, külföldi katonai múlt) miatt jóval erőszakosabbak, cselekvésüket a hadijogtól való teljes függetlenség jellemzi. Ez a hadifoglyokkal való kegyetlenebb bánásmódra és a lakosság tervszerű megfélemlítésére egyaránt jellemző. A lakosság közül szisztematikusan kiemelték a másik felet támogató irányadó politikai személyeket, a közintézményeket pedig fegyveresen megszállva tartották. A két fél kölcsönösen követett el az általa uralt területeken politikai gyilkosságokat, amellyel demoralizálta a helyi csoportokat, illetve letörte a politikai ellenállásukat, elejét véve egy felkelés elleni lázadásnak. A teljes cselekvési szabadsággal rendelkező felkelők többször megkínózták politikai áldozatukat, majd könnyen megtalálható helyre tették a holttestet. Külső támogatásra vall a klasszikus, szervezett formája az állami hatalmat jelképező személyek célzott likvidálása. Ennél is fontosabb, hogy a felkelők tervezett stratégiájuk részeként közvetítik azt a megszállt területen maradt kijevi támogatók felé, hogy az ukrán haderő a vezetőket sem tudja megvédeni. Ezek a politikai gyilkosságsorozatok Európában szintén Ukrajnában jelentek meg az aszimmetrikus hadviselés részeként, kamerák által jól dokumentálva, ezen eseményekkel később az orosz különleges műveleti erőknél szolgáló katonákat hozták összefüggésbe.²⁹ A két szembenálló fél háttérbázisát is jelentő Oroszországban, illetve Ukrajnában a fegyveres összeütközést ellenző, arról nyíltan kritikusan vélekedő politikusokat, újságírókat és rendőrtiszteket lőttek agyon, és végeztek ki autóba rejtett pokolgéppel.³⁰ A gyilkosságokhoz valószínűsíthető szélsőjobboldali, paramilitáris

²⁷ HEGEDŰS Henrik: Még egy front nyílt Ukrajnában. A focipályán., <http://www.origo.hu/sport/futball/20140313-az-ukran-futball-szinte-minden-futballklubjanak-jovoje-veszelyben-van.html> (Letöltés ideje 2017. 11. 10.)

²⁸ Coal Age: Ukrainian Coal: An Industry Divided, <http://www.coalage.com/features/4409-ukrainian-coal-an-industry-divided.html#.WGa3xBvhBPY> (Letöltés ideje: 2016. 12. 30.)

²⁹ BBC: Ukraine alert as politician killed, <http://www.bbc.com/news/world-europe-27118875> (Letöltés ideje: 2017. 01. 01.)

³⁰ BBC: Russia opposition politician Boris Nemtsov shot dead, <http://www.bbc.com/news/world-europe-31669061>. Bővebben: CHRISTOFOROU, Alex: Another Journalist Murdered in Ukraine. Body Count Hits 14 And Rising, <http://theduran.com/another-journalist-murdered-ukraine-body-count-hits-14-counting/> (Letöltés ideje: 2017. 01. 01.)

kötődést az orosz propaganda tényszerűvé teszi, ezáltal sikeresen agitál nemzetközi szinten is az ukrán kormány ellen, amivel a lázadó entitásokat erősíti a kisebbik rossz elve lapján.

A harcok elemzésénél kiemelném a helyi és a világsajtó tevékenységét. A konfliktus elején az ukrán szervezett állami és kormánypárti oligarchák által szigorúbb kontroll alatt tartott kereskedelmi médiáé volt a vezető információs, tájékoztató szerep. Az ukrán kormány a tradicionális propaganda-csatornákat használta, mint az újság, a televízió, rádió, kormányzati csatornák. Nem sikerült kihasználnia az internetben rejlő lehetőségeket, az angol nyelvű tájékoztatása gyenge volt. Nem sikerült megragadnia az ukrán diaszpórát mint humánerőforrást. Az ukrán kormány által végrehajtott külföldi toborzás az ukrán etnikumúak között jóval kisebb mértékű volt, mint az ellenség esetében. Ukrajnában rajtuk kívül érkeztek katonai múlttal igen, vagy azzal sem rendelkező amerikai, és más nyugati, esetleg keleti önkéntesek, de számuk jelzi, hogy a toborzásukban rejlő potenciált nem sikerült kiaknázni. Ukrajna a diaszpórát csak részben tudta felhasználni politikai céljainak érdekében, mivel az is megosztott volt. Ez az állam felé érzett korábbi, megtépzott lojalitás mellett a nem megfelelő propagandában gyökerezik, illetve az orosz dezinformációnak is köszönhető. Az ukrán haderő sikerei nem jutottak el hírek formájában megfelelően az átlagemberekhez. Európában és Ukrajnában is általánosan a haderő harctéri megítélése rossz, holott a komplett orosz egységek beavatkozásáig az ukrán haderő ütőképese csapatai jelentős sikereket értek el. A közösségi médiában döntően alulról, állampolgári, katonai állományból szerveződő kezdeményezések még most is jelen vannak az interneten közzé tett videók, képek formájában. A kijevi kormány hiába korlátozta az újságírók jelenlétét.

A felkelők kevés média-erőforrással rendelkeztek kezdetben, amit folyamatosan rendőrállami, erőszakon alapuló militarista állapotokkal (pl.: ellenőrző pontok, erős kontroll, befolyásolt igazságszolgáltatás) és nacionalista, demagóg propagandával próbáltak ellensúlyozni: szélsőjobboldalinak, korruptnak, romlott nyugati kapitalista bábkormányának beállítva a kijevi adminisztrációt. Oroszország a felkelés életképességének kezdeti megnyilvánulása után folytatta a folyamat gerjesztését, és mindennemű támogatást megadott, beleértve a nemzetközi politikai propagandát és médiamegjelenést. A felkelők nagyon ügyesen kihasználták a közösségi médiában rejlő lehetőségeket, ugyanis szervezeten rengeteg harci videót töltöttek fel, és több propagandaoldalt is üzemeltettek. A kilőtt ukrán járművek, elhagyott felszerelés, és sajnos elesettek is rengeteg fotósorozat témáját adták nekik, amiket előszeretettel töltöttek fel. Demonstratívák voltak a hadifoglyok vallatásáról, szégyenmenetéről, megalázásáról készült videók, amelyeken például a hírhedt „Motorola” becenévre hallgató Arsen Pavlov lázadó parancsnok szerepelt. Az ukrán haderő veszteségeit sikerrel tárták a közvélemény elé, amely együttesen az ukránokra is demoralizálólag hatott, és úgy tüntette fel az ukrán kormányt, mint amely elhallgatja a veszteségeket. Természetesen a szeparatisták donyecki videói a harcokról, kilőtt járművekről manipulatívák is lehetnek. Ennek ellenére rendkívül sok orosz, és más európai önkéntes csatlakozott hozzájuk. Nagy számukat tekintve sikeres toborzókampányról beszélhetünk. Értékelésem szerint a felkelők kiterjedt hálózatot üzemeltetnek, hisz több európai országban is megszervezik az önkéntesek utaztatását. Kimondhatjuk, hogy a jelenlegi patthelyzet a felkelőknek kedvez, ugyanis segít területi előnyüket megőrizni. Viszont az ukrán kormány társadalmi támogatottsága is adott a nagyhatalmi nyomásra létrejött fegyverszüneti

megállapodás után is a fegyveres ellenállás további folytatásához. A felkelők, melynek magját radikális, Oroszországhoz csatlakozni kívánó katonai elit alkotja, makacsul fog ragaszkodni céljaihoz. Harci tevékenységének jelenleg csak a Moszkva által állított fékek szabnak gátat. Mivel identitásalapú³¹ a konfliktus, a felkelők nem fogják feladni az Ukrajnától való függetlenedés gondolatát, mint alapvető célt.

Az orosz-ukrán fegyveres összetűzések

A hálózatalapú hadviselés részeként a felkelők élen jártak a kritikus infrastruktúra elleni támadások (kommunikáció, közlekedés), majd ideológiai, kulturális, puha célpontok elleni támadásokban, amelyekkel célzottan félemlítették meg az oroszpartii lakosságot. Az ukrán erők az érintett területek elszigetelésével, illetve klasszikus EÁP-ok felállításával próbálták korlátozni a mozgalom térnyerését, a különböző lázadók közötti kapcsolattartást.³² A legfontosabb a konfliktus kiszélesedése esetén a lakosság megvédése a lázadóktól, gondoskodni az állampolgárok biztonságáról. Ebben az időtényező miatt az ukrán biztonsági erők kudarcot vallottak. A szétzilált haderő többször nem kapott részletes, koordinált utasításokat, a felkelésellenes műveletek pedig elszigetelt ad-hoc jellegű intézkedéseket takartak, melyek közül sok kontraproduktív volt. A felkelők több kisebb támadással klasszikus módon a rendőrörsöket támadták meg a felszerelés miatt, illetve a helyi laktanyákat, raktárakat, kormányzati létesítményeket fosztották ki. Jellemző módon a többségében orosz etnikumú területeken a haderő megbízhatatlannak bizonyult: a rendőrség, illetve a katonák egy része nem avatkozott be, vagy átadta a fegyvereit, járműveket, és egyszerűen dezertált, vagy a felszerelésével és a kivezényelt alakulatával együtt csatlakozott a lázadókhöz. A felfegyverzett fegyveres csoportok így könnyedén hatalmukba keríthették a főbb csomópontokat, kommunikációs vonalakat, illetve az SZBU épületeket. A titkosszolgálat létesítményeinek korai elfoglalásával információs előnyhöz juthattak, illetve orosz kézre adhattak kulcsfontosságú információkat.³³

Kutatásaim szerint ezekben az akciókban diverzáns orosz katonai alakulatok is részt vehettek. Nem hozzáértőként is feltételezhetjük, hogy a felkelők információ terén előnyben voltak az ukrán erőkkel szemben, ugyanis vezetőik és katonáik egy része is a hivatásos orosz fegyveres erők tagja, így naprakész információkat kaptak a hírszerzéstől³⁴, gondolok itt az OSINT, SIGINT, HUMINT³⁵ teljes tárházára, illetve a legnaprakészebb műholdfelvételekre az ukrán csapatmozgásokról. Ez az

³¹ Bővebben: RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban, 2013.

³² KARMANAU, Yuras – The Associated Press: Ukraine launches operation against insurgents in the east, <http://www.ctvnews.ca/world/ukraine-launches-operation-against-insurgents-in-the-east-1.1790031> (Letöltés ideje: 2017. 10. 15.)

³³ KyivPost: Pro-Russian separatists say they will stay in Luhansk SBU building until their demands are met, <https://www.kyivpost.com/multimedia/photo/pro-russian-activists-seized-sbu-building-stay-inside-till-satisfaction-of-their-demands-343131> (Letöltés ideje: 2017. 09. 17.)

³⁴ KOBOLKA István (szerk.): Nemzetbiztonsági alapismeretek, 2013. Nemzeti Közszerzői és Tankönyv Kiadó Zrt., 2013., pp. 115-151.

³⁵ Bővebben: Információs Hivatal: HUMINT, <http://www.mkih.hu/humint.shtml> (Letöltés ideje: 2017. 09. 17.)

információs előny újszerű,³⁶ hiszen az általános az ukrán konfliktusig az volt, hogy a felkelőkkel szemben álló kormányzat és a hadsereg rendelkezik több információval. Ez még a hidegháború idején a nagyhatalmi támogatást élvező felkelő mozgalmakra sem volt jellemző. A szeparatisták hatalmukba kerítették több fontos települést: Kramatorszk, Druzszkovka, Horlivka, Mariupol, Jenakijeve. Az ukrán haderő április-július közötti ellentámadásaival sikerült visszafoglalni Mariupolt, Kramatorszkot, Szlavjanskot. Az oroszellenes tüntetéseket Luhanszk és Donyeck területek kivételével sikerült elfojtani.

Donyeckben és Luhanszkban viszont nem jártak sikerrel, ezzel elveszítve a két oblaszt Oroszországgal közös határszakasza fölötti ellenőrzést. Ebben a két megyében teljességgel kudarcot vallott a lakosság kontrollja, az ellenséges erők visszaszivárgásának a megakadályozása és a szeparatista államszervezet megsemmisítése. A helyi ukrán lakosság kitelepítése sem sikerült maradéktalanul a harcterről, amely csökkentette volna az áldozatok számát. A két oblaszt részben elvesztése felbátorította Oroszországot, hogy aktívan részt vegyen a konfliktusban, és növelje annak intenzitását.

Az ukrán erők a konfliktus során alapvetően a hadsereg, az SZBU speciális egységeire (Alfa Csoport) és a területiális védelmi erők alakulataira támaszkodtak.³⁷ Ezen katonai szervezetek közül kiemelendő volt a Kharkiv, Donbas, Dnipro-1, 79. Air Assault Brigade elnevezésűek, utóbbi a donyecki repülőtérért vívott harcok során kiérdemelte a „Cyborg” megnevezést. Az ukránok a rosszul felfegyverzett szeparatisták ellen sikerrel alkalmazták a légi szállítású csapatokat, a gépesített és harckocsidandárokat, és a nehézfegyverzetet. Kezdetben a közvetlen légi támogatás is hatékonynak bizonyult, ameddig nem állt a felkelők rendelkezésére nagy számú kézi, vállról indítható légvédelmi rakéta.³⁸ Az ukrán erőknek a hozzájuk húzó lakossággal sikerült együttműködni, ugyanakkor szükségleteit, ellátásukat nem tudták kellő módon biztosítani. A harcterről való kitelepítésükre is csak a leghévesebb harcokkal egyidőben került sor. Így nem sikerült elejét venni a polgári lakosság szükségtelen veszteségeinek. Az ukrán haderő ATO-nak, Anti Terrorist Operation-nek nevezte a műveletet. Az ATO-műveletekben oroszánrészt vállalt az SZBU a médiában pszeudo-műveleteknek nevezett harci cselekményekben. Ezek a csoportok a felkelők kohéziója megbontásának céljából hírszerzést, célmegjelölést, felderítést, elfogást, illetve célzott csoportok megsemmisítését végezte a frontvonal mindkét oldalán. (Az ukrán erőknek kritikus fontosságú feladata ma is a felkelők csoportjainak, illetve a formális, informális és orosz tanácsadói vezetés feltérképezése, illetve hogy elvágják a felkelők önkénteseinek és fegyverzetének beszivárgását Ukrajnába.) Rajtaütésekben sikerült kisebb csoportokat felszámolni,

³⁶ Bővebben: HAIG Zsolt: Az információbiztonság komplex értelmezése, http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.html (Letöltés ideje: 2017. 09. 17.)

³⁷ Divergent Options: Options to Arm Volunteer Territorial Defense Battalions in Ukraine, <https://divergentoptions.org/2017/03/02/arm-ukraine-battalion/> (Letöltés ideje: 2017. 09. 17.)

³⁸ Reuters: Special report: Where Ukraine's separatists get their weapons, <http://www.reuters.com/article/us-ukraine-crisis-arms-specialreport/special-report-where-ukraines-separatists-get-their-weapons-idUSKBN0FY0UA20140729> (Letöltés ideje: 2017. 09. 17.)

de az orosz jellegű állami szállítás kérdése még mindig nyitott volt.³⁹ A hasonló nyelv megkönnyíti mindkét félnek a beszivárgást a másik szervezeteibe, viszont ez veszélyesebb az ukrán félnek, hiszen őket érintette a sok átállás, amiben tevékeny része volt az FSZB-nek.⁴⁰ Ugyanakkor a különleges műveletek során a légi támogatás, a kiemelés lehetőségével egyértelműen előnyösebb helyzetbe hozták az ukrán erőket. Az ukrán haderőt kiegészítette több milícia-rendszerben működő önkéntes alakulat is. Ilyen az Azov és a Sich zászlóalj⁴¹, valamint több szélsőjobboldali félkatonai szervezet. Ezen egységek hűsége erősen kérdéses volt. A harcértékük a felszereléstől és az alegységek személyi állományának kiképzettségétől függött. Ezen alakulatok felfegyverzésével az erőszakmonopóliumot elvesztette az ukrán kormány, amely erősen csökkentette a legitimitását. Megítélésére rossz fényt vetett az európai támogatók körében a szélsőjobboldali, neonáci politikai tömbökhöz köthető fegyveres csoportok létezése. Ezek a csoportok többször nem rendelték magukat alá a hadsereg utasításainak, ugyanakkor rendelkeznek a legmodernebb ukrán haditechnikával, ilyen pl. a T-64BM1M harckocsi, amely kis számban állt rendelkezésre a hadsereg alakulatain belül is. Azóta fegyelem terén konszolidálódott a helyzet. Ezen szervezetek gyakorlatilag kontroll nélkül rendelkeznek a rájuk bízott fegyverzetrel, a harctéren elkövetett atrocitásaik pedig komoly problémák forrásai lehetnek a jövőben, ha valamilyen okból szembe fordulnának a kormánnyal. Az ukrán csapatoknál is harcoltak amerikai, európai, és nagyobb számban tatár és csecsen önkéntesek. Az ukrán haderő a harcok korai szakaszában megfelelő haditechnikai tartalékkal rendelkezett, a veszteségeit tudta pótolni. A 2014. április 9-től szeptemberig Donyeck és Luhanszk városáig nyomult előre, ami véleményem szerint főképp a szeparatisták rossz kiképzésének, és a korábban zsákmányolt nehézfegyverzet elvesztésének⁴² köszönhető, amelyet akkor még nem sikerült megfelelő mértékben pótolni. Külső segítség nélkül a szeparatisták hamarosan vereséget szenvedtek volna a reguláris haderőtől.

³⁹ IGCP: Security Service of Ukraine seized weapon from pseudo-volunteers going to the anti-terror operation region, <http://igcp.eu/en/news/34-security-service-of-ukraine-seized-weapon-from-pseudo-volunteers-going-to-the-anti-terror-operation.html> (Letöltés ideje: 2017. 01. 01.)

⁴⁰ MILLER, Christopher: Ukraine's top intelligence agency deeply infiltrated by Russian spies, <http://mashable.com/2014/12/30/russian-vs-ukrainian-spies/#GRv2FBd5NOqV> (Letöltés ideje: 2017. 10. 15.)

⁴¹ KLEIN, Margarete: RUFs Briefing No. 27: Ukraine's volunteer battalions – advantages and challenges <https://web.archive.org/web/20150624013217/http://www.foi.se/Documents/RUFs%20Briefing%20No.%2027%20.pdf> (Letöltés ideje: 2017. 11. 12.)

⁴² Reuters: Ukraine rebels cite heavy losses battling Kyiv troops <https://www.voanews.com/a/ukraine-rebels-cite-heavy-losses-battling-kyiv-troops/1940841.html> (Letöltés ideje: 2017. 11. 12.)



1. ábra: 2014. júliusában publikált helyzetkép Kelet-Ukrajnában, az ukrán hadsereg előretörése után⁴³

A szeparatista erők haditechnikai háttere

A szeparatista erők magját az oroszok, valamilyen szintű katonai kiképzéssel rendelkező személyek adták. A konfliktus elején megfigyelhető volt az idősebb korosztály részvétele a harcokban, majd később az állomány fiatalodása volt tapasztalható. Ez a helyi kiképzéssel egybekötött utánpótlás, majd a külföldi önkéntesek miatt változott meg. A szeparatistákhoz nagy számban csatlakoztak abház, orosz, fehérorosz, kazah önkéntesek. Az oroszok között egyformán megtalálható mind a szélsőbal és a szélsőjobb képviselői is. A harctevékenység szempontjából hírhedtté vált alakulatok: Vostok dandár, Oplot dandár (harckocsizó), Kalmius dandár, Sparta zászlóalj, Somalia zászlóalj, Prizrak dandár, Batlman zászlóalj és a Kozák Nemzeti Gárda főleg doni kozákokból. Az alakulatok az LPR (luhanszki) és a DPR (Donyecki Népköztársaság) alárendeltségébe tartoztak. A szeparatisták ukrán és orosz eredetű fegyverzettel rendelkeztek. Légierőjük nem volt, továbbá közepes, illetve nagy magasságban is hatásos légvédelmi fegyverzettel nem rendelkeztek. A fegyverzet elsősorban az ukrán zsákmányolt készletekből származott. Először 2014. június 11-én észlelték a műholdfelvételeken, hogy az orosz-ukrán határon csoportosított orosz haderő átlépte

⁴³ NSDC of Ukraine: The Situation in the Eastern Regions of Ukraine, http://www.rmbo.gov.ua/files/2014/RNBO_map_11_07_eng.jpg (Letöltés ideje: 2017. 11. 10.)

az ukrán határt.⁴⁴ Ezek a járműoszlopok zömében teherautókból, T-72B/B1, B obr. 1989/90g, B3 változatú harckocsikból, BMP-2 és egyéb, főként páncélozott, lánctalpas járművekből állt. Először a korábban tartalékba helyezett járművekről volt szó, majd az aktív alakulatok állományából is transzferáltak járműveket. Később az oroszok által lefoglalt krími készletekből is adtak át – oroszországi kiterővel – T-64BV harckocsikat. Az orosz csapatok megközelítőleg 300 volt ukrán harckocsit zsákmányoltak a Krímben, amelyeket rövid időn belül bevetésre alkalmas állapotba hozhattak.⁴⁵ Az orosz készletekből származó harcjárműveket legtöbb esetben teljesen vagy részben lefestették, a kocsitesten az azonosító jelzéseket, és a toronyszámokat megváltoztatták. Az átszállítás közben és a harcok alatt az átfestés különböző fázisaiban számos fotó készült a harcjárművekről, melyeken egyértelműen azonosíthatók, és nyomon követhető az útjuk.

Az orosz harckocsikra jellemző a kocsitesten a H2200 jelölés, amely az orosz 200. Gépesített Lövészandár jelölése.⁴⁶ Példaként (2. ábra) itt az Oplot zászlóalj egyik T-72B1 harckocsija, amely 318-as toronyszámmal és 'Viking' egyéni névvel erősíti a DNR kötelékét. Emellett a toronyládán az orosz 15. Független Gépesített Lövészandár jelzése látható alább.



2. ábra: T-72B1 DNR-318 'Viking' Oplot zászlóalj⁴⁷

A Krím-félszigeten 2014. február 20. és március 19. között a szevasztopoli katonai támaszpontonról beszivárgó egységek, az ún. „zöld emberkék” felségjelzés és rendfokozat nélküli egyenruhákban, azonosítatlan járművekkel minimális ellenállás

⁴⁴ Reuters: Ukraine accuses Russia of letting rebels bring in tanks, <http://www.reuters.com/article/us-ukraine-crisis-tanks-idUSKBN0EN1KS20140612> (Letöltés ideje: 2016. 11. 13.)

⁴⁵ Informnapalm.org: Guide to Russian T-64 tanks in Donbass: Part 1, <https://informnapalm.org/en/guide-russian-t-64-tanks-donbas-part-1/> (Letöltés ideje: 2016. 11. 13.)

⁴⁶ Bellingcat: Russia's 200. Motorized Infantry Brigade in the Donbass: The tell-tale tanks <https://www.bellingcat.com/news/uk-and-europe/2016/07/04/russias-200th-motorized-infantry-brigade-donbass-tell-tale-tanks/> (Letöltés ideje: 2017. 11. 12.)

⁴⁷ GRI AI: The Lost Legion: Tanks of the Oplot Battalion <https://informnapalm.org/en/the-lost-legion-tanks-of-the-oplot-battalion/> (Letöltés ideje: 2017. 11. 12.)

mellett elfoglalták a Krím-félszigetet, a lakosság jelentős hányadának támogatása mellett. Ugyan itt is sor került Ukrajna-párti tömegtüntetésekre, ahogy oroszbarát ellentüntetésekre is, a katonai erődemonstráció és az erőviszonyok voltak a döntőek. Az ukrán haderő a laktanyáiba zárkózott és később a fegyverzete hátrahagyása után Ukrajnába távozható. A repülőgépek egy része később visszaadásra került. Az ukrán flotta szintén nagyrészt passzívan vette tudomásul az orosz megszállást. Szervezett ellentevékenységre nem került sor. Valószínűleg nem spontán akció volt az ukrán zászlóshajó, a *Hetman Sahaidachny*⁴⁸ és még pár egység orosz kézre juttatása. Ezt valószínűleg előzetes titkosszolgálati kapcsolattfelvétel előzte meg. Véleményem arra alapozom, hogy átállt a frissen kinevezett flottaparancsnok, Sergei Yeliseyev és további két admirális, számos flotta hírszerző és magas beosztást ellátó tiszt a műveleti parancsnokságról. Az orosz különleges műveleti erők elfoglalták a krími parlamentet, valamint több, önálló nemzeti és államisági jelképet viselő, vagy szimbolikus jelentőségű közintézményt.⁴⁹ Ezzel klasszikusan az államiság jelképeit támadták, amiket azonnal el is távolítottak, ezzel demoralizálva a helyi lakosságot, illetve az új államhatalom státuszát fejezték ki. A krími annexió után Kelet-Ukrajnában is megjelentek a komplett, reguláris orosz zászlóalj harccsoportok, amelyek alkalmazásának fő célja a 2014 nyári ukrán előrenyomulás után a szeptatista vonal stabilizálása, majd az ukrán erők visszaszorítása és az ilovajszki katlan felszámolása voltak. Ekkorra már a szeptatisták vezetését is átvették a korábban az FSZB, vagy az orosz hadsereg alezredesi, ezredesi rendfokozatot elért katonái, zászlóalj és dandár szinten (Arsen Pavlov, Igor Bes) sok csecsenföldi veteránnal.⁵⁰ Az alakulatok személyi állománya az orosz különleges, légi szállítású, vagy képzett lövész erőinél szolgáló „civilekkel” került feltöltésre. Véleményem szerint az önkéntesek nagy száma és szervezethegye egyértelműen az orosz haderő fedett tevékenységét jelzi. A határon átdobott orosz alakulatok tisztességesen bántak a hadifoglyokkal, de a donyecki, és egyéb félkatonai orosz önkéntesek részéről rendszeresen lehetett hallani a hadifoglyok bántalmazásáról, lelövéséről, megszégyenítéséről.

A következő képen (3. kép) látható T-72B1 a debaltsevei katlancsatában vett részt, fotók alapján kikövetkeztethető források szerint az orosz 5. harckocsidandár részeként Vuglegirsnél, a járművön az e célra felfestett fehér négyzet különbözteti meg az orosz egységeket a szeptatista alakulatok közül. Mint a fehér karjelzés a zöld emberkéknél. Mindkét oldalon használnak viszonylag gyakran változtatott, de egyedi és egyszerű megkülönböztető jelzéseket. A cél az, hogy felismerjék a saját csapatokat, mivel a szembenálló feleknél használt fegyverzet megegyezik.

⁴⁸ RT: Ukrainian Navy flagship takes Russia's side – report –, <https://www.rt.com/news/ukraine-navy-flagship-protest-389/> (Letöltés ideje: 2016. 12. 29.)

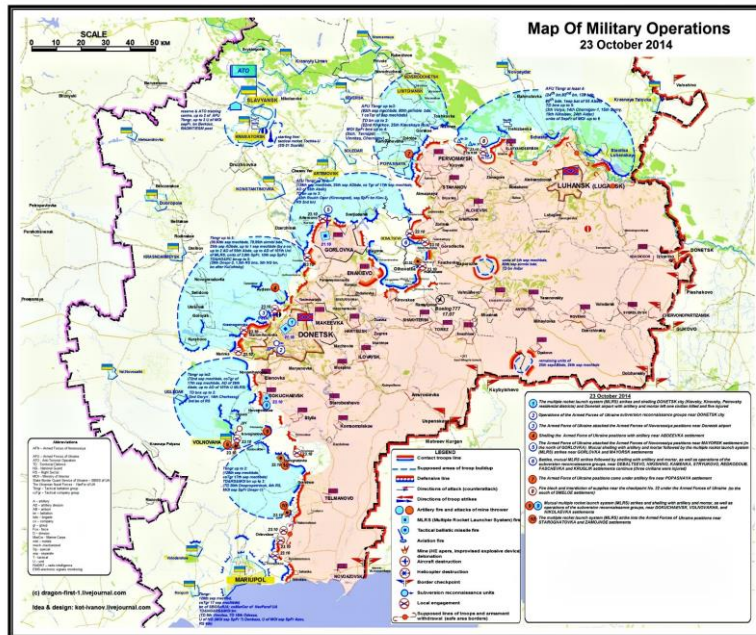
⁴⁹ Ukraine Today: Putin dedicates Russian 'Special Ops Forces Day' to date of 2014 Crimea parliament seizure, <http://uatoday.tv/news/putin-dedicates-russian-special-ops-forces-day-to-date-of-2014-crimea-parliament-seizure-412214.html> (Letöltés ideje: 2016. 12. 29.)

⁵⁰ BBC: Russian GRU military spy chief Igor Sergun dies, <http://www.bbc.com/news/world-europe-35226131> (Letöltés ideje: 2017. 01. 02.)



3. ábra: T-72B1 SvRF 5. hkdd Vuglegirsk, Debalceve
 Forrás: <http://mip.gov.ua/en/content/5a-tankova-brigda-vs-rf-v-boyah-za-debalceve.html>
 (Letöltés ideje: 2017. 10. 15.)

A következő két térképen (4. és 5. ábra) az orosz beavatkozás előtti, és az ellentámadást követő állapot látható:



4. ábra: 2014.10.23. Katonai műveletek Ukrajnában
 Forrás: <https://02varvara.wordpress.com/2014/10/24/24-october-2014-latest-sitrep-map-from-the-front-part-deux/> (Letöltés ideje: 2017. 10. 15.)



5. ábra: 2015.01.29. Katonai műveletek Ukrajnában
 Forrás: <http://www.chaussures2016.com/ukraine-war-map.html>
 (Letöltés ideje: 2017. 10. 15.)

Befejezés

Az ukrán konfliktus új megközelítésbe helyezte a hibrid hadviselés kérdéskörét, mely kapcsán az úgynevezett „Geraszimov doktrína” megkerülhetetlennek számít.⁵¹ Az Oroszországi Föderáció fegyveres erőinek vezérkari főnöke, Valerij Geraszimov tábornok 2013-ban publikált cikkében⁵² behatóan foglalkozik a 2010-2011-es „Arab tavasz” eseményeivel és a hadviselés terén bekövetkező változásokkal. Véleménye szerint annak egy teljesen új formája alakult ki az elmúlt években, mellyel kapcsolatban kifejti, hogy a katonai erő közvetlen bevetése helyett a jövőben sor kerül a politikai, gazdasági, diplomáciai és egyéb, nem katonai eszközök katonai erőkkel történő kombinált alkalmazására, létrehozva a hadviselés új formáját. A hadviselés ezen új formájában a reguláris, irreguláris és félkatonai erők rugalmas – *direkt és indirekt módszereket*⁵³ vegyítő – módon kerülnek alkalmazásra. Ezen túlmenően felhívta a figyelmet az információs hadszíntéren folytatott műveletek konfliktusokban játszott egyre növekvő

⁵¹ Bővebben: FEKETE Csanád: Információ és hadviselés, háború a kognitív hadszíntéren I. KNBSZ Szakmai Szemle 2016. 3. szám, http://knbsz.gov.hu/hu/letoltes/szsz/2016_3_szam.pdf; FEKETE Csanád: Információ és hadviselés, háború a kognitív hadszíntéren II. KNBSZ Szakmai Szemle 2016. 4. szám, http://knbsz.gov.hu/hu/letoltes/szsz/2016_4_szam.pdf (Letöltés ideje: 2017. 10. 15.)

⁵² GERASZIMOV, Valerij: Ценность науки в предвидении – Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, <https://www.vpk-news.ru/articles/14632> (Letöltés ideje: 2017. 10. 15.)

⁵³ Bővebben: RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés 2014.

jelentőségére. Ezek alkalmazása révén ugyanis számos aszimmetrikus lehetőség adódik az ellenség harci képességeinek csökkentésére, valamint általuk létrejön a csapatok közötti valós idejű koordináció. A tábormok szerint a jövő katonai műveleteiben kiemelkedő szerepe lesz az ellenség mélységében végrehajtott célzott csapásoknak, melynek során lerombolják annak kritikus információs infrastruktúráját, lebénítva a célország teljes kommunikációs rendszerét. A reguláris erők tényleges bevetésére a konfliktus kései szakaszában kerülne sor, így lehetőség nyílik azok tevékenységeit békefenntartó vagy válságkezelő műveleteknek álcázni. Geraszimov szerint e konfliktusokban kiemelt szerep hárul a különleges erőkre, mivel azok rendelkeznek azon képességekkel, melyek az ellenség által alkalmazott változatos módszereket – többek között a *rajtaütéseket* és a *merényleteket* – képesek ellensúlyozni.

Egy másik orosz szerző, Vladislav Szurkov – *Vlagyimir Putyin egyik tanácsadója* – 2014 márciusában megjelent cikkében az úgynevezett nemlineáris hadviselés elméletéről értekezik. A cikk a Krim-félszigeten kibontakozó meglepetésszerű műveleteket követően jelent meg, melyben a hibrid hadviseléshez hasonló koncepció kerül megfogalmazásra. Oroszország hivatalosan nem építette be katonai dokumentumaiba a leírtakat, de a tábormok és Szurkov által kifejtett módszerek egyes elemei tetten érhetőek a krími válság során folytatott műveletekben. Az ukrainai eseményeket követően olyan vélemények jelentek meg, hogy az oroszok kidolgozták saját hibrid hadviselésre vonatkozó stratégiájukat, melynek gyakorlatba történő átültetését jelenleg is tesztelik Kelet-Ukrajnában. Az eseményekben szerepet kaptak a konvencionális és nem konvencionális hadviselés elemei és az érdekérvényesítés egyéb formái. Ezek vizsgálatából megállapítható, hogy a krími beavatkozás során az oroszok nem léptek át egy bizonyos határt és végig kontroll alatt tartották az eseményeket, mely során hatékonyan kombinálták a különleges műveleteket és az információs hadviselés részeként folytatott dezinformációs és propaganda tevékenységeket. Mindez nem meglepő, tekintve, hogy az oroszok nagy gyakorlattal rendelkeznek a stratégiai megtévesztés (*maszkirovka*) és a lélektani műveletek (*reflexív kontroll*) terén.⁵⁴

Napjainkban Ukrajnában a minszki tűzszünet van érvényben, így felfüggesztették a nagyobb támadó hadműveleteket. Azonban a konfliktus befagyott jellege ellenére a tűzszünet törékenysége miatt bármikor kiújulhatnak és eszkalálódhatnak a harcok. Kisebb, helyi összecsapások rendszeresen zajlanak a harcoló felek között. Ilyenek közül a legjelentősebb a 2017. január 29. – február 4. között Avdiivka-nál tüzérség és harckocsik részvételével zajló harcok. A nehézfegyverzet szinte azonnali bevetése jelzi, hogy a megállapodás nehézfegyverzetre vonatkozó hátravonását sem tartják be a felek. Az összecsapások a település peremvonala mellett az Almaz-2 (Gyémánt) álláspont ukrán elfoglalása miatt robbantak ki, és amely több, kudarcba fulladt szeparatista ellentámadást tartalmazott. Mindkét oldalon több tucat halálos áldozattal és sérülttel jártak a

⁵⁴ Bővebben: FEKETE Csanád: Információ és hadviselés, háború a kognitív hadszíntéren I. KNBSZ Szakmai Szemle 2016. 3. szám, http://knbsz.gov.hu/hu/letoltes/szsz/2016_3_szam.pdf – FEKETE Csanád: Információ és hadviselés, háború a kognitív hadszíntéren II. KNBSZ Szakmai Szemle 2016. 4. szám (Letöltés ideje: 2016. 11. 13.)

harcok.⁵⁵ A harcok alatt orosz részről ismételt alkalommal alkalmazták a pszichológiai hadviselés eszközeit: az ukrán katonák mobiltelefonjaikra ismeretlen számokról demoralizáló, megfélemlítő üzeneteket kaptak.⁵⁶ A magántelefonszámokhoz való hozzáférés a titokvédelem elégtelenségét jelzi. Az Almaz-2 pontért vívott harcok alatt jelentős veszteséget szenvedett a Donyecki és a Luhanszki Népköztársaság is. Valószínűleg megtorlásképp az ukrán különleges műveleti erők követték el Oleg Anaschenko luhanszki védelmi miniszter felrobbantását autóba rejtett pokolgéppel.⁵⁷ Napokkal később vállról indítható rakétával az irodájában kilőtték Mikhail 'Givi' Tolstykh-ot, a Somalia zászlóalj parancsnokát. Givi a felkelés kezdetétől egyik kulcsfontosságú vezetője volt a szeparatista erőknek, és a hadifogyokkal való bánásmód miatt keresett háborús bűnös.⁵⁸ Mindkét vezető az Avdiivka-i harcok helyszínén tartózkodott. Jelentős eseményként értékeltem a 2017 júniusában indult Petya vírusátadást⁵⁹, amely a továbbra is magas intenzitású kiberműveletekre világít rá. Az irányított műveletek elsősorban a kritikus ukrán pénzügyi, közlekedési, kormányzati és gazdasági rendszereket vették célba. Az SZBU ezt a támadást⁶⁰ észak-koreai és orosz eredetűnek tartja, mint a korábbi, azonos módszereket alkalmazó támadásokat a TeleBots és BlackEnergy esetében.⁶¹ Politikailag Oroszország és Ukrajna álláspontja nem közeledett egymáshoz, így belátható időn belül irreleváns a konfliktus rendezésére.

Véleményem szerint az ukrán konfliktus, az abban alkalmazott orosz módszerek a hadviselés egy olyan formáját mutatják meg, amely kitölti a hidegháborús tömeghadseregek alkalmazása közötti és az iraki, afganisztáni gerilla hadviselés közötti koncepciót. Ez lehet a jövőben a legalkalmasabb katonai jellegű felfogás egy ország destabilizálására professzionális haderővel, illetve a dezinformációval, hálózatalapú hadviseléssel, megfelelő titkosszolgálati tevékenységgel és a média alkalmazásával karöltve.⁶² Ez jelentősen csökkentheti a veszteségeket, és politikailag sokkal nagyobb nyomás alá lehet helyezni vele egy országot, és a körülötte elterülő régiót.

⁵⁵ KRAMER, Andrew E. Residents Take Cover as Ukraine Border Battles Reignite Conflict, https://www.nytimes.com/2017/02/03/world/europe/ukraine-russia-conflict-avdiivka.html?_r=0 (Letöltés ideje: 2017. 11. 03.)

⁵⁶ MILLER, Christopher: 'Our Tanks Are Ready': Ukraine Braces For Escalation In Eastern War, <https://www.rferl.org/a/ukraine-avdiyivka-fighting-escalation/28276963.html> (Letöltés ideje: 2017. 11. 03.)

⁵⁷ BBC: Ukraine conflict: Rebel commander killed in bomb blast, <http://www.bbc.com/news/world-europe-38868600> (Letöltés ideje: 2017. 11. 03.)

⁵⁸ The Associated Press: Separatist commander Mikhail Tolstykh, 'Givi' killed in eastern Ukraine, <http://www.cbc.ca/news/world/separatist-commander-mikhail-tolstykh-givi-killed-ukraine-1.3971740> (Letöltés ideje: 2017. 11. 03.)

⁵⁹ POLITYUK, Pavel: Ukraine points finger at Russian security services in recent cyber attack, <http://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P> (Letöltés ideje: 2017. 11. 03.)

⁶⁰ SBU Press-center: SBU establishes involvement of the RF special forces services into Petya.A virus-extorter attack, <https://ssu.gov.ua/en/news/1/category/21/view/3660#.UFcIDLG8.dpbs> (Letöltés ideje: 2017. 11. 03.)

⁶¹ BORYS, Christian: Ukraine braces for further cyber-attacks, <http://www.bbc.com/news/technology-40706093> (Letöltés ideje: 2017. 11. 03.)

⁶² SIMON László: Az információ, mint fegyver? KNBSZ Szakmai Szemle 2016. 1. szám, http://www.knbsz.gov.hu/hu/letoltes/szsz/2016_1_szam.pdf (Letöltés ideje: 2017. 10. 15.)

Felhasznált irodalom:

- BALMFORTH, Richard – Reuters: Ukraine’s new rulers disband riot police, <http://www.reuters.com/article/us-ukraine-crisis-berkut-idUSBREA1P0AK20140226> (Letöltés ideje: 2016. 10. 16.)
- BALOGH Fatime - FEKETE Csanád – NÉMETH András – NÉMETH József Lajos: A hibrid hadviselés különös tekintettel a mobil kommunikációra, http://www.hadmernok.hu/154_12_balogf_na_joe.pdf (Letöltés ideje: 2017. 10. 15.)
- BORYS, Christian: Ukraine braces for further cyber-attacks, <http://www.bbc.com/news/technology-40706093> (Letöltés ideje: 2017. 11. 03.)CHRISTOFOROU, Alex: Another Journalist Murdered in Ukraine. Body Count Hits 14 And Rising, <http://theduran.com/another-journalist-murdered-ukraine-body-count-hits-14-counting/> (Letöltés ideje: 2017. 01. 01.)
- DEARDEN, Lizzie: Vladimir Putin issues executive order recognising documents issued by separatists ‘republics’ in Ukraine, <http://www.independent.co.uk/news/world/europe/vladimir-putin-donald-trump-ukraine-war-crimea-rebels-separatists-executive-order-documents-donetsk-a7587666.html> (Letöltés ideje: 2017. 09. 17.)
- FEKETE Csanád: Információ és hadviselés, háború a kognitív hadszíntéren I. KNBSZ Szakmai Szemle 2016. 3. szám, http://knbsz.gov.hu/hu/letoltes/szsz/2016_3_szam.pdf, (Letöltés ideje: 2017. 10. 15.)
- FEKETE Csanád: Információ és hadviselés, háború a kognitív hadszíntéren II. KNBSZ Szakmai Szemle 2016. 4. szám, http://knbsz.gov.hu/hu/letoltes/szsz/2016_4_szam.pdf (Letöltés ideje: 2017. 10. 15.)
- GERASZIMOV, Valerij: Ценность науки в предвидении – Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, <https://www.vpk-news.ru/articles/14632> (Letöltés ideje: 2017. 10. 15.)
- HAIG Zsolt: Az információbiztonság komplex értelmezése, http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.html (Letöltés ideje: 2017. 09. 17.)
- HAIG Zsolt: Információ Társadalom Biztonság, NKE Szolgáltató Kft., 2015. pp. 292. ISBN: 978-615-552-708-1
- HEGEDŰS Henrik: Még egy front nyílt Ukrajnában. A foci pályán., <http://www.origo.hu/sport/futball/20140313-az-ukran-futball-szinte-minden-futballklubjanak-jovoje-veszelyben-van.html> (Letöltés ideje 2017. 11. 10.)
- KARMANAU, Yuras – The Associated Press: Ukraine launches operation against insurgents in the east, <http://www.ctvnews.ca/world/ukraine-launches-operation-against-insurgents-in-the-east-1.1790031> (Letöltés ideje: 2017. 10. 15.)

- KEMÉNY János: A felkelésellenes hadviselés lakossággközpontú elméletének fejlődése a XX-XXI. században, http://phd.lib.uni-corvinus.hu/769/1/Kemeny_Janos.pdf (Letöltés ideje: 2017. 10. 15.)
- KLEIN, Margarete: RUFBS Briefing No. 27: Ukraine's volunteer battalions – advantages and challenges <https://web.archive.org/web/20150624013217/http://www.foi.se/Documents/RUFBS%20Briefing%20No.%2027%20.pdf> (Letöltés ideje: 2017. 11. 12.)
- KOBOLKA István (szerk.): Nemzetbiztonsági alapismeretek. Nemzeti Közszoelgálati és Tankönyv Kiadó, 2013. ISBN 978-615-5344-32-9
- KRAMER, Andrew E.: Residents Take Cover as Ukraine Border Battles Reignite Conflict, https://www.nytimes.com/2017/02/03/world/europe/ukraine-russia-conflict-avdiivka.html?_r=0 (Letöltés ideje: 2017. 11. 03.)
- MILLER, Christopher: 'Our Tanks Are Ready': Ukraine Braces For Escalation In Eastern War, <https://www.rferl.org/a/ukraine-avdiivka-fighting-escalation/28276963.html> (Letöltés ideje: 2017. 11. 03.)
- MILLER, Cristopher: Ukraine's top intelligence agency deeply infiltrated by Russian spies, <http://mashable.com/2014/12/30/russian-vs-ukrainian-spies/#GRv2FBd5NOqV> (Letöltés ideje: 2017. 10. 15.)
- POLITYUK, Pavel: Ukraine points finger at Russian security services in recent cyber attack, <http://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P> (Letöltés ideje: 2017. 11. 03)
- RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés – Kis háborúk nagy hatással. Zrínyi Kiadó, 2014. pp. 421. ISBN: 9789633275924
- SIMON László: Az információ, mint fegyver? KNBSZ Szakmai Szemle 2016. 1. szám, http://www.knbsz.gov.hu/hu/letoltes/szsz/2016_1_szam.pdf (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: BBC News: Ukraine crisis: Timeline, <http://www.bbc.com/news/world-middle-east-26248275> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: BBC: Russia opposition politician Boris Nemtsov shot dead, <http://www.bbc.com/news/world-europe-31669061> (Letöltés ideje: 2017. 01. 01.)
- Sz.n.: BBC: Russian GRU military spy chief Igor Sergun dies, <http://www.bbc.com/news/world-europe-35226131> (Letöltve: 2017. 01. 02.)
- Sz.n.: BBC: Ukraine alert as politician killed, <http://www.bbc.com/news/world-europe-27118875> (Letöltés ideje: 2017. 01. 01.)
- Sz.n.: BBC: Ukraine conflict: Rebel commander killed in bomb blast, <http://www.bbc.com/news/world-europe-38868600> (Letöltés ideje: 2017. 11. 03.)

- Sz.n.: Bellingcat: Russia's 200. Motorized Infantry Brigade in the Donbass: The tell-tale tanks <https://www.bellingcat.com/news/uk-and-europe/2016/07/04/russias-200th-motorized-infantry-brigade-donbass-tell-tale-tanks/> (Letöltés ideje: 2017. 11. 12.)
- Sz.n.: CFR.org: Budapest Memorandums on Security Assurances, 1994., <http://www.cfr.org/nonproliferation-arms-control-and-disarmament/budapest-memorandums-security-assurances-1994/p32484> (Letöltés ideje: 2016. 10. 25.)
- Sz.n.: Coal Age: Ukrainian Coal: An Industry Divided, <http://www.coalage.com/features/4409-ukrainian-coal-an-industry-divided.html#.WGa3xBvhBPY> (Letöltés ideje: 2016. 12. 30.)
- Sz.n.: Dailymail: <http://www.dailymail.co.uk/news/article-3195711/Now-CHILDREN-taking-arms-Shocking-pictures-inside-Ukraine-s-neo-Nazi-military-camp-recruits-young-six-learn-fire-weapons-s-ceasefire.html> (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: Divergent Options: Options to Arm Volunteer Territorial Defense Battalions in Ukraine, <https://divergentoptions.org/2017/03/02/arm-ukraine-battalion/> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: EBESZ: Minsk Declaration, <https://www.oscepa.org/documents/all-documents/annual-sessions/2017-minsk/declaration-25/3555-declaration-minsk-eng/file> (Letöltés ideje 2017. 09. 17.)
- Sz.n.: EEAS: Questions and Answers about the East StratCom Task Force, http://collections.internetmemory.org/haeu/content/20160313172652/http://eea.s.europa.eu/top_stories/2015/261115_stratcom-east_qanda_en.htm (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: EP Hírek: Az Európai Parlament ratifikálta az EU és Ukrajna közti társulási szerződést, <http://www.europarl.europa.eu/news/hu/news-room/20140915IPR62504/az-eur%C3%B3pai-parlament-ratifik%C3%A1lta-az-eu-%C3%A9s-ukrajna-k%C3%B6zti-t%C3%A1rsul%C3%A1si-szerz%C5%91d%C3%A9st> (Letöltés ideje: 2016. 10. 16.)
- Sz.n.: EP Hírek: Kronológia az ukrainai eseményekről, <http://www.europarl.europa.eu/news/hu/news-room/20140203STO34645/kronol%C3%B3gia-az-ukrainai-esem%C3%A9nyekr%C5%91l> (Letöltés ideje: 2016. 10. 16.)
- Sz.n.: Euromaidan Press: Ukraine targeted by disinformation campaign to restore "friendship" with Russia, <http://euromaidanpress.com/2017/01/12/fake-news-campaign-in-ukraine-presses-to-restore-economic-relations-with-russia/#arvldata> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: Híradó.hu: Három éve ért véget Ukrajnában a forradalom <https://www.hirado.hu/2017/02/22/harom-eve-ert-veget-ukrajnaban-a-forradalom/?source=hirkereso> (Letöltés ideje: 2017. 09. 17.)

- Sz.n.: IGCP: Security Service of Ukraine seized weapon from pseudo-volunteers going to the anti-terror operation region, <http://igcp.eu/en/news/34-security-service-of-ukraine-seized-weapon-from-pseudo-volunteers-going-to-the-anti-terror-operation.html> (Letöltés ideje: 2017. 01. 01.)
- Sz.n.: Információs Hivatal: HUMINT, <http://www.mkih.hu/humint.shtml> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: Informnapalm.org: GRI AI: The Lost Legion: Tanks of the Oplot Battalion <https://informnapalm.org/en/the-lost-legion-tanks-of-the-oplot-battalion/> (Letöltés ideje: 2017. 11. 12.)
- Sz.n.: Informnapalm.org: Guide to Russian T-64 tanks in Donbass: Part 1, <https://informnapalm.org/en/guide-russian-t-64-tanks-donbas-part-1/> (Letöltés ideje: 2016. 11. 13.)
- Sz.n.: ISD Dunaferr: Együtt a jövőbe, <http://www.dunaferr.hu/hu/> (Letöltés ideje: 2016. 12. 30.)
- Sz.n.: KyivPost: Pro-Russian separatists say they will stay in Luhansk SBU building until their demands are met, <https://www.kyivpost.com/multimedia/photo/pro-russian-activists-seized-sbu-building-stay-inside-till-satisfaction-of-their-demands-343131> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: MTI: Amerikai páncélos dandár jön Kelet-Európába, <http://www.hirado.hu/2016/03/30/amerika-egy-pancelos-dandart-telepit-kelet-europaba/> (Letöltés ideje: 2016. 10. 16.)
- Sz.n.: MTI: Megérkezett Lengyelországba a NATO nemzetközi zászlóaljának első kontingense, http://www.nyugat.hu/tartalom/cikk/134932_megerkezett_lengyelorszagba_a_nato_nemzetkozi_első (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: NATO: Ukraine cooperation in the military sphere, <http://nato.mfa.gov.ua/en/ukraine-nato/military> (Letöltés ideje: 2016. 10. 25.)
- Sz.n.: NATO: Relations with Ukraine, http://www.nato.int/cps/en/natolive/topics_37750.htm (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: NSDC of Ukraine: The Situation in the Eastern Regions of Ukraine, http://www.rnbo.gov.ua/files/2014/RNBO_map_11_07_eng.jpg (Letöltés ideje: 2017. 11. 10.)
- Sz.n.: Nyugat.hu: http://www.nyugat.hu/tartalom/cikk/134932_megerkezett_lengyelorszagba_a_nato_nemzetkozi_első (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: Reuters: Special report: Where Ukraine's separatists get their weapons, <http://www.reuters.com/article/us-ukraine-crisis-arms-specialreport/special-report-where-ukraines-separatists-get-their-weapons-idUSKBN0FY0UA20140729> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: Reuters: Ukraine accuses Russia of letting rebels bring in tanks, <http://www.reuters.com/article/us-ukraine-crisis-tanks-idUSKBN0EN1KS20140612> (Letöltés ideje: 2016. 11. 13.)

- Sz.n.: Reuters: Ukraine rebels cite heavy losses battling Kyiv troops <https://www.voanews.com/a/ukraine-rebels-cite-heavy-losses-battling-kyiv-troops/1940841.html> (Letöltés ideje: 2017. 11. 12.)
- Sz.n.: RT: Ukrainian Navy flagship takes Russia's side – report –, <https://www.rt.com/news/ukraine-navy-flagship-protest-389/> (Letöltés ideje: 2016. 12. 29.)
- Sz.n.: SBU Press-center: SBU establishes involvement of the RF special forces services into Petya.A virus-extorter attack, <https://ssu.gov.ua/en/news/1/category/21/view/3660#.UFcIDLG8.dpbs> (Letöltés ideje: 2017. 11. 03.)
- Sz.n.: The Associated Press: Separatist commander Mikhail Tolstykh, 'Givi' killed in eastern Ukrain, <http://www.cbc.ca/news/world/separatist-commander-mikhail-tolstykh-givi-killed-ukraine-1.3971740> (Letöltés ideje: 2017. 11. 03.)
- Sz.n.: TiszaNews.org.ua: Több mint 10 fegyveres rejtőzködik Munkácsnál, <http://tiszaneews.org.ua/?module=news&&target=get&id=8774> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: Ukraine Today: Putin dedicates Russian 'Special Ops Forces Day' to date of 2014 Crimea parliament seizure, <http://uatoday.tv/news/putin-dedicates-russian-special-ops-forces-day-to-date-of-2014-crimea-parliament-seizure-412214.html> (Letöltés ideje: 2016. 12. 29.)
- Sz.n.: Unian.info: Humanitarian intervention as basis for using force against another nation, <https://www.unian.info/world/1104120-humanitarian-intervention-as-basis-for-using-force-against-another-nation.html> (Letöltés ideje: 2017. 09. 17.)
- Sz.n.: <http://mip.gov.ua/en/content/5a-tankova-brigda-vs-rf-v-boyah-zadabalceve.html> (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: <https://02varvara.wordpress.com/2014/10/24/24-october-2014-latest-sitrep-map-from-the-front-part-deux/> (Letöltés ideje: 2017. 10. 15.)
- Sz.n.: <http://www.chaussures2016.com/ukraine-war-map.html> (Letöltés ideje: 2017. 10. 15.)
- SZENTIRMAI Péter: Az ukrán válság katonai oldalának új kihívásai OTDK, Budapest 2017.
- VARGA Tamás: Az orosz-ukrán gázvita, http://kitekinto.hu/europa/2009/01/08/az_orosz-ukran_gazvita (Letöltés ideje: 2017. 11. 08.)
- VENDRICZKI Gábor – Ukrajna: NATO-tagság, vagy sem? – http://kitekinto.hu/europa/2015/10/19/ukrajna_nato-tagsag_vagy_sem (Letöltés ideje: 2016. 10. 25.)

Bevezetés

A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény¹ (a továbbiakban: Hvt.) egyes rendelkezéseinek végrehajtásáról szóló 290/2011. (XII. 22.) Korm. rendelet 22. § (2) bekezdése alapján a Kormány határozza meg a honvédelemben közreműködő szervek által készítendő terveket és azok tartalmi követelményeit. A védelmi igazgatás tervrendszerének bevezetéséről szóló 1061/2014. (II. 18.) Korm. határozat² 1. pont d) alpontjában a Kormány felkérte a Magyar Nemzeti Bank (a továbbiakban: MNB) elnökét, hogy szakterületét érintően működjön együtt az MNB-re vonatkozó honvédelmi intézkedési terv kidolgozásával és bevezetésével összefüggő feladatok végrehajtásában.

A Magyar Nemzeti Bank szerepe a védelmi igazgatás rendszerében

Magyarország gazdasági és pénzügyi rendszerének stabilitása és ellenálló képessége fontos nemzeti érdek és biztonságpolitikai szempont. Magyarország Nemzeti Biztonsági Stratégiája³ szerint a biztonság ma egyre átfogóbb értelmezést nyer, elengedhetetlenné vált a biztonság politikai, katonai, gazdasági, pénzügyi és társadalmi dimenziójának együttes kezelése. Egyre inkább előtérbe kerülnek azok a biztonságpolitikai kihívások, amelyek kezeléséhez átfogó és összehangolt politikai, gazdasági és – szükség esetén – katonai fellépésre van szükség. A tartós és fenntartható fejlődés alapvető követelménye a biztonság és a stabilitás, amely megköveteli a válságkezelési – beleértve a fejlesztéspolitikai – eszközök átfogó, és egyben egymással összhangban lévő használatát, az integrált civil-katonai megközelítést és képességfejlesztést. A nemzeti biztonsági stratégia csak valamennyi közreműködő szervezet részvételével és felelősségével, az intézményi keretek kihívásoknak való megfeleltetésével lehet hatékony és sikeres. A közreműködő intézmények felelőssége, hogy saját szakterületén állandó jelleggel értékelje a fenyegetettséget, és megtegye a szükséges lépéseket azok kezelésére és elhárítására.

Magyarország alapvető biztonsági érdekei közé tartozik az ország gazdasági stabilitásának és fejlődésének biztosítása is. Fel kell készülni arra, hogy térségünkben már nem is annyira a hagyományos fegyverekkel végrehajtott katonai támadás a legfőbb veszélyforrás, hanem a gazdasági, pénzügyi, energiabiztonsági, ellátási és környezeti veszélyeztetettség (összességében az aszimmetrikus

¹ A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény

² A védelmi igazgatás tervrendszerének bevezetéséről szóló 1061/2014. (II. 18.) Korm. határozat

³ Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat

hadviselés⁴ elemei a meghatározóak). Az instabil régiók, az államok közötti és államokon belüli konfliktusok, a gyenge vagy működésképtelen államok – amelyek így kevésbé képesek korlátok közé szorítani agresszív érdekérvényesítő csoportokat – potenciális veszélyt jelentenek Magyarország számára.

A pénzügyi stabilitás kérdése a 2008-2009-es világgazdasági válság hatására jelentősen felértékelődött. Hazánk sebezhetőségét nagymértékben csökkenti, ha sikeres az adósságcsökkentés, a külföldi kitétség mérséklése, a devizaadósság csökkentése, a gazdasági növekedés feltételeinek megteremtése. Magyarország biztonságának szilárd gazdasági alapokon kell nyugodnia, amely egyfelől megteremti a hatékony biztonságpolitika erőforrásait, másfelől pedig az ország stabilitásának fokozása révén növeli az ország érdekérvényesítő képességét.

Alapvető biztonságpolitikai cél a gazdasági és pénzügyi stabilitás folyamatos erősítése és felügyelete, a makroprudenciális szabályozás (rendszerszintű kockázatok folyamatos monitorozása és minél hatékonyabb kezelése) erősítése, a nemzetgazdaság külső kockázati kitétségének csökkentése, a társadalom jólétének megalapozott, biztonságos és hosszú távú erősítése.

A biztonság nem-katonai vetületeinek fontossága

A biztonság nem-katonai vetületeinek egyre inkább megnő a fontossága. Az Alaptörvénnyel összhangban Magyarország Nemzeti Katonai Stratégiája⁵ is rögzíti, hogy a honvédelem nemzeti ügy, amelynek két alappilléret a nemzeti önerő és a szövetségi együttműködés alkotják. Tekintettel arra, hogy a biztonság összetett és elemei szorosan összefüggnek egymással, a honvédelem ügyét nem lehet a biztonság más területeitől elválasztva, önmagában értelmezni. A biztonsági kihívások kezelése túlnyúlik az egyes intézmények hatáskörén, összehangolt együttműködést kíván meg az állami szereplőktől.

Elsősorban gazdasági és demográfiai változások történtek a világban, amelyek egyes Európán kívüli térségek felértékelődéséhez vezettek, és ezáltal Európa relatív súlyvesztése következett be. A pénzügyi, gazdasági világválság csökkentette az EU kohézióját, így fontosabbá vált a biztonsági struktúrák felülvizsgálata.

A globalizáció kihívásaihoz nehezen alkalmazkodó vagy alkalmazkodni képtelen államok, illetve térségek stabilitása törekeny, a gazdasági folyamatok kiszámíthatatlan irányt vettek, ami erősíti a nemzetközi terrorizmus bázisát, valamint a tömeges migráció által keltett veszélyek forrása is lehet. Az anarchiába süllyedt, működésképtelenné vált államok fenyegetést jelenthetnek az adott régió stabilitására, továbbá menedéket és kiképző terepet nyújthatnak a globális törekvésekkel bíró terrorista csoportok számára. A válságok kizárólag katonai erővel nem kezelhetők, kezelésük összetett civil és katonai erőfeszítést, együttműködést igényel, különös tekintettel az azonos műveleti területen működő katonai és polgári szakemberek egymásra utaltságára. A katonai és a civil erőfeszítések nem

⁴ RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban, Zrínyi Kiadó 2014., ISBN: 9789633275924, pp. 173-190.

⁵ Magyarország Nemzeti Katonai stratégiájának elfogadásáról szóló 1656/2012. (XII. 20.) Korm. határozat

választhatóak el élesen egymástól. A művelési területen nem csupán állami, hanem számos nem állami szereplő is meghatározó módon van jelen.

A honvédelem nemzeti ügy, ezért a honvédelem irányító szervei és a Honvédség feladatai mellett fontos szerep töltenek be a honvédelemben közreműködésre köteles szervezetek, amelyek jogszabály által meghatározottak szerint részt vesznek a honvédelmi feladatok ellátásában.

A Magyar Nemzeti Bank (továbbiakban: MNB) is a honvédelemben közreműködésre köteles szervezetek közé tartozik. A honvédelmi feladatok megvalósításában önkéntes alapon részt vesznek a társadalmi szervezetek – együttműködve a helyi védelmi igazgatás szerveivel, önkéntesség alapján elsősorban az országvédelem jelentőségének tudatosításával, a társadalom szerveinek és az állampolgároknak erre történő mozgósításának elősegítésével kapcsolatos feladatokban működnek közre, átfogják a lakosság széles rétegeit.

A honvédelem nemzeti ügy, az Alaptörvény kimondja, hogy hazánk polgárainak és az államnak közös célja a jó élet, a biztonság, a rend, az igazság, a szabadság kiteljesítése. A rend alapja a nemzet együttműködése.

A 21. században szükséges a gazdasági, társadalmi élet területeit érintő megújulás. Az európai népek szabadságának, jólétének és biztonságának kiteljesedése érdekében közreműködünk az európai egység megteremtésében – ennek megteremtése és megőrzése, valamint az emberiség fenntartható fejlődése érdekében együttműködésre törekszük a világ valamennyi nemzetével. A haza védelme minden magyar állampolgár kötelessége, valamint honvédelmi és katasztrófavédelmi feladatok ellátása érdekében – sarkalatos törvényben meghatározottak szerint – mindenki gazdasági és anyagi szolgáltatás teljesítésére kötelezhető.

Az Észak-atlanti Szerződéshez való csatlakozásunk következményeként az ország egyéni védelmi képességének fenntartása és fejlesztése mellett fontos a Washingtoni Szerződés szerinti kollektív védelmi képesség fenntartása, fejlesztése is. Hazánk a nemzeti és szövetségi védelmi képességének fenntartásában saját erejére – a nemzetgazdaság erőforrásaira, a Honvédség felkészültségére, valamint az állampolgároknak a haza védelme iránti hazafias elkötelezettségére és áldozatkészségére –, továbbá a szövetséges államok és fegyveres erőik együttműködésére és segítségnyújtására épít.

Az MNB hozzájárulása az ország stabilitásának, gazdasági, pénzügyi rendjének biztosításához

Magyarország Nemzeti Biztonsági Stratégiájának egyik kulcseleme az ország stabilitásának, gazdasági, pénzügyi rendjének biztosítása. Az Alaptörvény a közpénzekekről szóló címben szabályozza az MNB státuszát, feladatait. Az MNB hazánk központi bankja, így felelős a monetáris politikáért, valamint ellátja a pénzügyi közvetítőrendszer felügyeletét.

A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény⁶ részletesen meghatározza az MNB jogállását, szervezetét, elsődleges célját, alapvető és egyéb feladatait. Emellett rögzíti, hogy az MNB elsődleges célja az árstabilitás elérése és fenntartása, valamint ezen elsődleges céljának veszélyeztetése nélkül az MNB támogatja a pénzügyi közvetítőrendszer stabilitásának fenntartását, ellenálló képességének növelését, a gazdasági növekedéshez való fenntartható hozzájárulásának biztosítását és a rendelkezésére álló eszközökkel a Kormány gazdaságpolitikáját.

A védelmi igazgatás rendszere Magyarországon

A Hvt. egyes rendelkezéseinek végrehajtásáról rendelkező 290/2011. (XII. 22.) Korm. rendelet⁷ (Hvr.) 1. § n) pontjában foglalt meghatározás szerint „*a védelmi igazgatás a közigazgatás részét képező feladat- és szervezeti rendszer, amely az állam védelmi feladatainak megvalósítására létrehozott, valamint e feladatra kijelölt közigazgatási szervek által végzett végrehajtó, rendelkező tevékenység; magában foglalja a különleges jogrendre történő felkészülést, továbbá az említett időszakok és helyzetek honvédelmi, polgári védelmi, katasztrófavédelmi, védelemgazdasági, lakosság-ellátási feladatainak tervezésére, szervezésére, a feladatok végrehajtására irányuló állami tevékenységek összességét*”. A honvédelmi igazgatás a védelmi igazgatás része: feladat- és szervezetrendszer, melynek keretében az ország védelmére létrehozott, az e feladatra kijelölt közigazgatási szervek, és a honvédelemben közreműködő más szervek ellátják a honvédelemre való felkészítésével, az ország védelmével, és a honvédelmi kötelezettségek teljesítésével kapcsolatos feladatokat.

A biztonság fogalma

A biztonság⁸ az egyik legalapvetőbb emberi szükséglet. Egy állam belső biztonsága a politikai, társadalmi és gazdasági rend megővését, a veszélyek elkerülését, illetve elhárítását jelenti. A biztonság komplex jellegű, amelynek főbb dimenziói közé az alábbiak sorolhatók: katonai és védelmi, politikai, környezeti, gazdasági, társadalmi, szociális és információs biztonság. A gazdasági biztonság a nemzetgazdaság normál működését és növekedését jelenti. A védelmi tervezés célja az, hogy a nemzeti biztonsági stratégiában meghatározott feladatok végrehajtásához rendelkezésre álljanak a szükséges katonai és civil képességek. A nem katonai képességek létrehozása a tárcaközi együttműködés útján valósul meg.

A biztonsági kockázatokat katonai és nem katonai eszközökkel lehet kezelni. Azt, hogy mikor melyiket alkalmazzuk, a nemzeti védelempolitika határozza meg. Ebből adódóan a védelempolitikának nem csak a katonai képességek fenntartásával és fejlesztésével kell foglalkoznia, hanem a polgári ágazati képességekkel is, hiszen az ország védelméhez valamennyi erőforrást mozgósítani kell, de a békeidőben jelentkező biztonsági kockázatok kezelésére is készen kell állnia valamennyi polgári

⁶ A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény

⁷ A honvédelmi törvény egyes rendelkezéseinek végrehajtásáról rendelkező 290/2011. (XII. 22.) Korm. rendelet

⁸ CSER Orsolya: Értékmegőrzés válság idején a pénzügyintézeteknél
http://193.224.76.4/download/konyvtar/digitgy/publikacio/cser_orsolya01.pdf (Letöltés ideje: 2017. 11. 14.)

ágazatnak. A védelmi műveletekben a katonai erőknek integrálniuk kell a különböző civil szervezeteket, annak érdekében, hogy minél hamarabb helyreállítsák az adott állam működését (átfogó megközelítés – comprehensive approach). Az integrációs folyamat során nagyon komplex az érdek-, a működési mechanizmus, a hatékonyság, a hatáskör és jogkör különbözőség az egyes – katonai és civil – szereplők között.

A védelmi igazgatás komplex tervrendszere

A védelmi igazgatás tervrendszerének bevezetéséről szóló 1061/2014. (II. 18.) Korm. határozat⁹ 1. sz. mellékletében meghatározottak szerint a honvédelem, a katasztrófavédelem és a védelemgazdaság sajátos, egymástól funkcionálisan eltérő követelményeire tekintettel megfelelő tervdokumentáció kidolgozása indokolt. A védelmi igazgatási komplex tervrendszer része a különleges jogrendre történő felkészülés, és az ezzel kapcsolatos honvédelmi, polgári védelmi, katasztrófavédelmi, védelemgazdasági, lakosság-ellátási feladatok tervezése, szervezése, a feladatok végrehajtására irányuló tevékenységek összessége.

A komplex védelmi igazgatási terv a mai kor követelményeinek megfelelő, feladatorientált, a központi, területi és helyi sajátosságokat, továbbá a biztonságra hatást gyakorló kihívásokat (kockázatokat és veszélyforrásokat) maximálisan figyelembe vevő, a gyakorlatban jól használható, egymásra épülő, az együttműködést kiemelten kezelő tervrendszer.

A komplex tervrendszer biztosítja a különleges jogrend időszakában (megelőző védelmi helyzet, rendkívüli állapot, szükségállapot, veszélyhelyzet, az országot ért váratlan támadás), valamint a mindennapi életviszonyokat jelentős mértékben befolyásoló események bekövetkezése esetén is a honvédelemben közreműködő szervek vezetetségét, feladatainak ellátását, így az ország működőképességének fenntartását, szükség esetén a lakosság élet- és vagyonmentését, valamint a lakosság folyamatos ellátását. Szakmai, tartalmi követelményeit a honvédelmi igazgatási tervre vonatkozóan a honvédelemről, valamint a különleges jogrendben bevezethető intézkedésekről szóló jogszabályok; a veszély-elhárítási tervvel összefüggésben a katasztrófavédelmi jogszabályok; a védelemgazdasági alaptervvel kapcsolatban pedig a nemzetgazdaság védelmi felkészítését szabályozó jogszabályok határozzák meg.

A honvédelmi intézkedési terv célja és tartalma

A honvédelmi intézkedési terv célja, hogy Magyarország Alaptörvényében meghatározott rendkívüli állapot, szükségállapot, megelőző védelmi helyzet, vagy váratlan támadás (a továbbiakban: honvédelmi típusú különleges jogrend) idején – az adott körülmények által lehetővé tett mértékben – biztosítsa az MNB jogszabályban meghatározott feladatainak végrehajtására való képességét.

A honvédelmi intézkedési terv meghatározza a honvédelmi típusú különleges jogrend időszakában az MNB különleges működési rendjének szabályait, amely az

⁹ A védelmi igazgatás tervrendszerének bevezetéséről szóló 1061/2014. (II. 18.) Korm. határozat

MNB működésének fenntartása érdekében bevezetett intézkedéseket és eljárásokat, a meghagyási feladatokat, speciális biztonsági intézkedéseket, a munkavállalók kiértékelésére, berendelésére és készenléthez helyezésére, az ügyeleti szolgálat létrehozására és működtetésére, továbbá a kapcsolattartás megszervezésére vonatkozó rendelkezéseket foglalja magába.

A honvédelmi intézkedési tervvel kapcsolatos feladatok

A honvédelmi intézkedési terv elkészítéséért, naprakész állapotban tartásáért, és az érintett munkavállalóknak a honvédelmi intézkedési tervben foglaltakra való felkészítéséért a bankbiztonságért felelős szervezeti egység vezetője felelős. A honvédelmi intézkedési tervben foglaltak végrehajtásának elrendeléséről a Kríziskezelő Irányító Bizottság dönt.

A honvédelmi típusú különleges jogrend idején az Alaptörvény rendelkezései szerint kivételes hatalom – rendeleti kormányzás – érvényesül. A Hvt. meghatározza azokat a rendkívüli intézkedéseket, amelyeket szükségállapot idején a köztársasági elnök, rendkívüli állapot idején a Honvédelmi Tanács, megelőző védelmi helyzet vagy váratlan támadás esetén a Kormány rendeleti úton vezethet be.

A NATO Válságreakálási Rendszerrel összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről szóló 278/2011. (XII. 20.) Korm. rendeletben meghatározottak szerint a Nemzeti Intézkedési Rendszer keretében bevezetett intézkedések vezethetők be, amelyek végrehajtásában az MNB, mint honvédelemben közreműködő szerv a feladatköre szerint közreműködik. A rendkívüli intézkedések bevezetése és alkalmazása okán az ország személyi és dologi erőforrásai a haza fegyveres katonai védelme vagy az alkotmányos rend megóvása érdekében a szükséges mértékben igénybe vehetők. Ezek az intézkedések biztosítják az ország egész területén a közrend és közbiztonság fenntartását, valamint a lakosság védelmét és alapvető életszükségleteinek folyamatos kielégítését.

Gazdasági és anyagi szolgáltatási kötelezettség és mentességek

Az MNB a Hvt. 18. § (2) bekezdése szerint honvédelmi felkészülés egyes feladatainak ellátásában vesz részt. Az MNB-nek a védelmi igazgatás komplex rendszerében betöltött szerepe tekintetében, a gazdasági és anyagi szolgáltatási kötelezettség körében a honvédelmi feladatok szükségessé teszik az ország összes erőforrásának honvédelmi célokra való igénybevételét. Mind a természetes személyek, mind a jogi személyek gazdasági és anyagi szolgáltatásra kötelezhetők az Alaptörvény XXXI. Cikkének (6) bekezdése alapján honvédelmi és katasztrófavédelmi célból. Az MNB a Hvt. 15. § (1) bekezdés a) pontja alapján mentes a gazdasági és anyagi szolgáltatási kötelezettség alól. A mentességi szabályok és a mentesítettek körének meghatározásával a Hvt. elősegíti a társadalmi-politikai intézményrendszer zavartalan működését, illetve a lakosság alapellátásához nélkülözhetetlen közellátási, közszolgáltatási funkciók fenntartását.

Az üzletmenet-folytonosság biztosítása

Az MNB Igazgatóságának tagjaiból álló Kríziskezelő Irányító Bizottság (a továbbiakban: KIB) irányítja az MNB munkaszervezetét az üzletmenet folytonosságot veszélyeztető, az üzletmenet-folytonossági terv részleges vagy teljes aktiválását megkövetelő működési kockázati események következményeként kialakult helyzetben, krízishelyzetben.

A honvédelmi típusú különleges jogrend időszaka is krízishelyzet. Krízishelyzetben a munkaszervezetben belül a KIB a legmagasabb döntési joggal rendelkező szerv. A szakterületekre háruló operatív feladatokat krízishelyzetben a szakterületi kríziscsoportok látják el. A folyamatos működés krízishelyzetben történő fenntartása érdekében az MNB kidolgozta és elektronikus tervrendszerbe foglalta krízishelyzet-kezelési eljárásait (MNB üzletmenet-folytonossági terv).

A KIB – áttekintve az adott krízishelyzet kiterjedtségét – dönt az üzletmenet-folytonossági terv aktiválásáról, ide értve a teljes, minden szervezeti egységre kiterjedő aktiválást is, döntést hoz az alternatív helyszínre való kiköltözésről, valamint minden egyéb, a krízishelyzettel összefüggésben elé terjesztett – más testület vagy személy hatáskörébe nem tartozó – kérdésről. Az üzletmenet-folytonossági terv egyes akcióterveinek aktiválását (részleges aktiválás) a szakterületi kríziscsoport-vezetők, illetve a szervezeti egység-vezetők vagy felettes vezetők is elrendelhetik.

A részleges aktiválásról, az elrendelő haladéktalanul értesíti a felettes vezetőjét és a szakterület felett vezetői jogokat gyakorló KIB-tagot. Amennyiben a KIB nem ülészik, az operatív irányítást, a részleges aktiválást elrendelő szervezeti egység szerint feladatkörrel rendelkező igazgatósági tag, vagy az általa kijelölt vezető végzi. A KIB működésének szabályait az egyes belső működési kérdésekről szóló elnöki utasítás, valamint az MNB Működési kockázat kezelési kézikönyvről szóló alelnöki utasítás határozza meg.

Az MNB – közvetlen és közvetett – kizárólagos tulajdonában álló gazdasági társaságok

Az MNB feladatainak ellátásához kapcsolódik az MNB – közvetlen és közvetett – kizárólagos tulajdonában álló gazdasági társaságok tevékenysége, amelyre az MNB a honvédelmi típusú különleges jogrend idején is számít. Az MNB megteszi azokat a tulajdonosi joggyakorlás körébe tartozó intézkedéseket, amelyek ezen gazdasági társaságok honvédelmi típusú különleges jogrendi időszakban történő feladatellátását elősegítik.

A 290/2011. (XII. 22.) Korm. rendelet 1. számú mellékletében foglaltak alapján az MNB kizárólagos tulajdonában álló gazdasági társaságok az illetékes védelmi bizottság által egyedi határozattal kijelölhetők a meghagyásba bevont szervek közé.

Az MNB, mint a honvédelmi rendszer része

A Hvr. 16. §-a szerint a honvédelmi feladatok végrehajtására irányítási és vezetési rendszer szolgál, amelynek részei – a központi, területi és helyi államigazgatási és védelmi igazgatási szerveken kívül – a honvédelmi felkészítés egyes feladataiban részt vevő szervezetek, így az MNB is. A honvédelmi irányítási rendszerben résztvevő szervezeteknél honvédelemmel foglalkozó szervezeti egységet kell kijelölni.

Az MNB a Kormány honvédelmi igazgatási tárgykörökben kiadott határozataiban foglalt felkérése alapján, törvényi feladatköréhez igazodva részt vesz a honvédelmi igazgatási feladatokban¹⁰:

- a védelmi tervezés rendszerének kialakítása, működtetése, intézkedési terv elkészítése;
- a nemzetgazdasági erőforrások honvédelmi célú tartalékolása, a gazdaságfelkészítési tervezése;
- az ország területének hadművelati előkészítéséből adódó feladatok;
- a feladat- és hatáskörébe tartozó különleges jogrendi intézkedések előkészítése:
 - a NATO Válságreakálási Rendszerrel összhangban álló, feladat- és hatáskörébe tartozó nemzeti intézkedések, rendszabályok végrehajtása,
 - az eseményfigyelő- és jelzőrendszer működtetése;
- a honvédelmi felkészülés irányítási, szervezeti, működési rendszer kialakítása, feltételek biztosítása;
- a szervezetet érintő honvédelmi feladatok gyakorlása, a gyakorlatokon való részvétel tervezése;
- a tárgyévet megelőző év honvédelmi feladatainak végrehajtásáról és az e célra jóváhagyott költségvetési források felhasználásáról szóló beszámolás (november 30.), valamint a honvédelmi felkészítés következő évi feladattervének és a szükséges költségvetési igényeknek összeállítása;
- a jogszabályban vagy kormányhatározatban részére megállapított honvédelmi feladatok elvégzése.

A honvédelmi típusú különleges jogrendi időszak kihirdetése esetén feladatellátásban résztvevő munkavállalók eljárásainak alapelvei:

- jelen vannak a számukra a feladatellátásra meghatározott helyszínen;
- egymással együttműködve, fegyelmezetten, az útmutatásoknak megfelelően látják el feladataikat;
- támogatják egymást a rendkívüli helyzet okozta fizikai, lelki stresszhelyzet kezelésében;
- kölcsönösen megosztják egymással a feladatellátáshoz szükséges információkat;
- a nemzetközi és hazai – polgári, katonai, rendvédelmi – hatóságokkal a vonatkozó előírások szerint együttműködnek, támogatják azok feladatellátását;
- a feladatellátás áttekinthető, hatékony, a lehetőséghez képest dokumentált és nyomon követhető;

¹⁰ Az MNB honvédelmi ágazati intézkedési terve

- törekednek a hosszú távú gondolkodásra, a rendkívüli helyzetet követő időszak előkészítésére, hogy a helyreállítás minél gyorsabb és eredményesebb lehessen;
- feladatellátása nem ér véget a rendkívüli körülmények elmúltával, biztosítani kell a helyreállításhoz, a normál működéshez szükséges feltételeket is;
- megelőző intézkedéseket hajtanak végre – a rendkívüli időszakra történő felkészülés, és a feladatellátás idején –, hogy a káros következmények az adott körülmények között a legkisebbek legyenek.

Az MNB-ben alkalmazandó intézkedések honvédelmi típusú különleges jogrendi időszak esetén:

1. A szervezeti egység-vezető (a személyügyekért felelős szervezeti egység vezetőjének bevonásával)

- előkészíti a munkavállalókat érintő korlátozó és szigorító intézkedések szükség szerinti bevezetését
- rendkívüli munkavégzés (ügyeleti szolgálat) elrendelése;
- a munkavállaló lakóhely elhagyásának bejelentési kötelezettsége;
- a munkavállaló lakáson készenlétben való tartózkodás elrendelése;
- a munkavállaló állandó elérhetőségének biztosítása;
- a fizetett szabadság felfüggesztése, a szabadidő és a pihenőidő korlátozása.
- gondoskodik a szabadságon, kiküldetésben tartózkodók névsorának összeállításáról [(név, szervezeti egység, munkakör, távozott (mikor, hová, meddig), elérhető (cím, telefon))];
- javaslatot tesz a távol lévő munkavállalók szükség szerinti visszarendelésére, a munkaidőn túli tartózkodási hely bejelentésére, illetve a lakáson készenlétben állás elrendelésére, felkészül a szabadságon lévők, illetve az egyéb okból távollévők visszarendelésének előkészítésére;
- intézkedik a szolgálati utak minimálisra korlátozására;
- szabadságot csak különösen indokolt esetben engedélyezhet,
- biztosítja az irányítása alatt álló munkavállalóknak a feladataik ellátásához szükséges információkat, és hogy megismerjék a honvédelmi típusú különleges jogrend idején hatályba lépő jogszabályokat;
- az irányítása alatt álló szervezeti egység feladatköre vonatkozásában folyamatosan elemzi a kialakult helyzetet, és feladatkörét érintően megteszi a szükséges intézkedéseket, illetve javaslatokat a végrehajtandó feladatokra.

2. A bankbiztonságért felelős szervezeti egység vezetője

- intézkedik a védelmi igazgatási ügyeleti szolgálat felállításáról;
- gondoskodik az egyéni védőeszközök állapotának ellenőrzéséről, illetve szükség szerinti kiosztásáról és a használat elrendeléséről;
- gondoskodik az MNB őrzés-védelmének szükség szerinti átszervezéséről, az MNB objektumai védelmének megerősítéséről;
- gondoskodik a folyamatos kapcsolattartásról a központi és a területi védelmi igazgatás szervekkel;

- az MNB munkahelyi polgári védelmi szervezetének közreműködésével gondoskodik a fegyveres összeütközések időszakában végrehajtandó polgári védelmi feladatok ellátásáról;
- gondoskodik a vezetők tájékoztatásáról a kihirdetett vagy kinyilvánított honvédelmi típusú különleges jogrendi helyzettel kapcsolatos védelmi igazgatási, honvédelmi információkról;
- gondoskodik az ügyeleti szolgálatban résztvevő munkavállalók – adott helyzetnek megfelelő – védelmi felkészítéséről és szükség szerint védőfelszereléssel történő ellátásáról;
- gondoskodik a védelmi igazgatási szakfeladatok, különösen a központi, területi és helyi védelmi igazgatási szervekkel való együttműködéssel, a HIKOM munkájával, a mozgósítással, a befogadó nemzeti támogatással kapcsolatos feladatok elvégzéséről;
- a személyügyekért felelős szervezeti egység vezetőjének közreműködésével gondoskodik a meghagyási jegyzék aktualizálásáról, illetve hadkötelezettség bevezetése esetén az aktualizált jegyzék alapján elkészíti a meghagyási névjegyzéket, amelyet elküld a Magyar Honvédség katonai igazgatási és központi adatfeldolgozó szervének;
- intézkedik a telefonközpont – indokoltság esetén – 24 órás, folyamatos üzemeltetéséről;
- a tapasztalt rendkívüli eseményekről, az azokkal összefüggésben tudomására jutott információkról azonnali tényközlő jelentést készít a KIB részére.

A honvédelmi típusú különleges jogrendben hatályba lépő jogszabályi előírásoknak megfelelően, a bankbiztonságért felelős szervezeti egység vezetőjének kezdeményezésére a jogi ügyekért felelős szervezeti egység koordinálásával, haladéktalanul el kell végezni a belső szabályok, tervek és eljárásrendek módosítását.

3. MNB munkahelyi polgári védelmi szervezetének parancsnoka intézkedik
 - az MNB munkavállalóinak közellátási utalványokkal való ellátásáról;
 - az életvédelemmel kapcsolatos védőeszközök készenlétbe helyezéséről, szükség szerinti pótlólagos beszerzéséről, illetve a szükséges egyéni és kollektív védelem (utóbbi keretében elzárkózásra alkalmas helyiség vagy szükségóvhely) biztosításáról, használatra előkészítéséről.
4. A működésikockázat-kezelésért felelős szervezeti egység vezetője koordinálja
 - a szakterületi ügyeleti rendszer felülvizsgálatát, és a szolgálat megerősítését, azokon a szakterületeken, ahol ügyeleti rendszer nem működik, és az elrendelt feladatok indokolják.
5. A kormányzati koordinációért felelős szervezeti egység vezetője gondoskodik
 - a vezetők tájékoztatásáról a különleges jogrend idején kihirdetett jogszabályokról.
6. A kommunikációért felelős szervezeti egység vezetője biztosítja
 - a hír-, média-, sajtó és a közszolgálati média műsorainak folyamatos figyelemmel kísérését.

7. Az üzemeltetésért felelős szervezeti egység vezetője gondoskodik
- a bankbiztonságért felelős szervezeti egység polgári védelmi és katasztrófavédelmi szakközreműködése mellett a munkavállalók soron kívüli munka- és tűzvédelmi oktatásának végrehajtásáról;
 - a bankbiztonságért felelős szervezeti egység vezetőjével együttműködve azon szolgáltatási igények pontosításáról, amelyeket a nemzetgazdasági készletekből az MNB működéséhez biztosítani kell;
 - az igényelt nemzetgazdasági szolgáltatásokat kezdeményezéséről;
 - a 24 órás gépjármű ügyeletről és a szolgálatok pihentetésének és ellátásának feltételeiről.

A védelmi igazgatási ügyeleti szolgálat

A védelmi igazgatási ügyeleti szolgálat céljai az alábbiakban kerülnek felsorolásra, melynek elrendelése különleges jogrendi időszakban rendkívüli fontossággal bír. A KIB feladatainak honvédelmi típusú különleges jogrend idején történő támogatását, a honvédelmi feladatok és a válságkezelés feladatai szervezett megkezdését, a védelmi igazgatási szervekkel való kapcsolattartást, továbbá a bekövetkezett vagy várhatóan bekövetkező eseményekre való reagálás koordinálását védelmi igazgatási ügyeleti szolgálat látja el.

A védelmi igazgatási ügyeleti szolgálat elrendeléséről, valamint visszavonásáról – a bankbiztonságért felelős szervezeti egység vezetőjének kezdeményezésére – a KIB dönt. Az ügyeleti szolgálat munkahelyre berendelt rendelkezési állományának pihentetéséről és ellátásáról az üzemeltetésért felelős szervezeti egység vezetője gondoskodik. Az ügyeleti szolgálat elhelyezési feltételeit, a személyek étkezési ellátását, a működést támogató hírközlési, telekommunikációs és irodai eszközöket, személygépkocsit és személygépkocsi-vezetőt az üzemeltetésért felelős szervezeti egység vezetője, az informatikai eszközöket az informatikáért felelős szervezeti egység vezetője biztosítja.

A védelmi igazgatási ügyeleti szolgálat ellátása folyamatos, 24 órás (váltások 08:00 órakor), és egy váltásban egyszerre 6 fő ad szolgálatot az MNB Székház kijelölt irodáiban:

- a bankbiztonságért felelős szervezeti egység vezetője vagy a helyettesítésére kijelölt személy,
- a bankbiztonságért felelős szervezeti egység védelmi igazgatási szakterületének vezetője vagy a helyettesítésére kijelölt személy,
- a bankbiztonságért felelős szervezeti egység őrzésvédelmi és biztonságtechnikai szakterületének vezetője vagy a helyettesítésére kijelölt személy,
- a bankbiztonságért felelős szervezeti egység vezetője által a bankbiztonságért felelős szervezeti egység állományából kijelölt további személy,
- 1 fő asszisztens, és 1 fő gépkocsivezető.

Az ügyeleti szolgálat a bankbiztonságért felelős szervezeti egység vezetőjének – vagy helyettesének – közvetlen alárendeltségében végzi feladatát. A szolgálat vezetőjének akadályoztatása esetén feladatkörét a szolgálat legmagasabb beosztású tagja külön utasítás vagy felhatalmazás nélkül átvenni köteles; több azonos beosztású tag esetén az idősebb vezető.

A szolgálat ellátása során legalább két személynek mindig az ügyeleti helyiségekben kell tartózkodnia. A szolgálat tagjainak folyamatosan biztosítani kell az állandó mobiltelefonos összeköttetés lehetőségét. A szolgálatot ellátók a munkaidőn kívüli tevékenységükért külön díjazásban részesülnek, térítésmentes étkezésre jogosultak.

A védelmi igazgatási ügyeleti szolgálat feladatai

- kapcsolattartás az MNB felsővezetőivel és a védelmi igazgatási feladatokban közreműködő szervezetekkel,
- az általános ügyeleti rendszer keretében beérkező információk, utasítások vétele, ennek alapján intézkedések megtétele, az MNB felsővezetőinek tájékoztatása, tőlük utasítás kérése,
- az ügyeleti szolgálat vezetője a szolgálat ideje alatt történt rendkívüli eseményeket jelenteni köteles az MNB felsővezetőinek és a közreműködő védelmi szerveknek, így különösen:
 - az ország biztonságát vagy közrendjét érintő eseményt,
 - emberi életet kioltó vagy súlyon veszélyeztető elemi csapást, balesetet vagy támadást,
 - az MNB objektumait ért jelentősebb károsodást,
 - nagyobb tüzesetet,
 - közművek szolgáltatásainak általános és tartós kimaradását,
 - minden olyan egyéb információt, amely jelentőségénél fogva intézkedést igényel.

A védelmi igazgatási ügyeleti szolgálatba beosztott személy kötelezettségei

- tanulmányozni és elsajátítani a szolgálati előírásokat, továbbá az eligazítás és a szolgálat átvétele után az abban foglaltakat végrehajtani,
- jelentési kötelezettségének folyamatosan – a vezető által meghatározott módon – eleget tenni,
- a szolgálat átvétele után ellenőrizni:
 - a legszükségesebb hírösszeköttetés feltételeinek meglétét, működőképességét,
 - a technikai eszközök üzemképességét,
 - a futárszolgálatba beosztottak kiértesíthetőségét,
 - a munkavégzéshez szükséges együttműködő szervezeti egységekkel és külső szervezetekkel való kapcsolattartást,
- fel kell készülnie az érkező jelzések, jelentések vételére, továbbítására, a kapott feladatok végrehajtására,
- szolgálati naplót kell vezetnie, melybe be kell jegyeznie:
 - a szolgálati ideje alatt történt eseményeket,
 - a vezetőtől kapott és az általa kiadott utasításokat, intézkedéseket,
 - az együttműködő szervezetek vezetőinek jelentéseit,
 - a végrehajtott ellenőrzéseket.
- haladéktalanul jelentenie kell a szolgálat vezetőjének:
 - a körülményekben észlelt bármilyen érdemi változást,
 - a riasztás, illetve a kiértesítés végrehajtását,

- az életet, testi épséget, anyagi javakat fenyegető veszélyhelyzetet, vagy károsodást,
- bármilyen kár, veszteség, hátrány esetén azok megszüntetésére, illetve hatásának mérséklésére, csökkentésére tett intézkedéseket,
- azon eseményeket, melyek jelentésére utasítást kapott,
- minden eseményt, amely a megítélése szerint vezetői intézkedést, KIB döntést igényel.

Az ügyeleti szolgálatot ellátó személy ruházata az évszaknak és az időjárásnak megfelelő polgári öltözet vagy polgári védelmi ruházat és felszerelés, valamint szükség esetén egyéni védőeszköz.

Következtetések

Az Magyar Nemzeti Bank honvédelmi ágazati feladata a védelmi célú tartalékolásnak, mint állami feladatnak az egyik nagyon fontos eleme. Ennek biztosítása nagy mennyiségű forrást igényel mindazon képességek elérésénél, amelyek a nemzetgazdaság normál működésének időszakában nem, vagy csak korlátozottan érvényesülő szükségleteken alapszanak. A finanszírozásnál külön kezelendők a tartalékkészletek fejlesztésével, átstrukturálásával járó – egyedi döntésen alapuló – felhalmozási kiadások és a tartalékolás fenntartásával (az infrastruktúra és a személyzet működtetésével, a készletek nyilvántartásával, ellenőrzésével) járó működési költségek.

Általánosságban az éves költségvetésben a tartalékok készletfejlesztésével, átstrukturálásával kapcsolatos költségeket a védelmi felkészítés központi kiadásai nemzetgazdasági minisztériumi fejezeti előirányzatból kell biztosítani. Ennek felosztásáról külön kormányzati döntést kell hozni – a védelmi felkészítés éves feladattervében meghatározottak szerint. A tartalékolás fenntartási költségeit a felelős tárca költségvetésben célszerű tervezni, illetve amennyiben az adott tartalék jellegéből következően erre lehetőség van, a szükséges forrásokat a tartalékkezelő szervezet gazdálkodási bevételeiből lehet részben vagy egészben fedezni.

Az MNB nagy előnye, hogy nem központi költségvetési szerv, így nem költségvetési forrásból gazdálkodik – ugyanakkor nagy stratégiai szerepe van a pénztartalékok képzésében és annak kezelésében. Jelentős saját forrásból gazdálkodóként a honvédelmi ágazati feladatait is sokkal magasabb színvonalon képes a jövőben ellátni, megoldani.

Felhasznált irodalom:

- RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban, Zrínyi Kiadó 2014., ISBN: 9789633275924
- CSER Orsolya: Értékmegőrzés válság idején a pénzügyintézeteknél http://193.224.76.4/download/konyvtar/digitgy/publikacio/cser_orsolya01.pdf (Letöltés ideje: 2017. 11. 14.)

Felhasznált jogforrások:

- A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény
- A védelmi igazgatás tervrendszerének bevezetéséről szóló 1061/2014. (II. 18.) Korm. határozat
- Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat
- Magyarország Nemzeti Katonai stratégiájának elfogadásáról szóló 1656/2012. (XII. 20.) Korm. határozat
- a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény
- a honvédelmi törvény egyes rendelkezéseinek végrehajtásáról rendelkező 290/2011. (XII. 22.) Korm. rendelet
- a védelmi igazgatás tervrendszerének bevezetéséről szóló 1061/2014. (II. 18.) Korm. határozat
- az MNB honvédelmi ágazati intézkedési terve

DEÁK VERONIKA

BIZTONSÁGTUDATOSSÁG AZ INFORMÁCIÓS KÖRNYEZETBEN

Az utóbbi években egyre intenzívebbé váltak a kibertámadások az állami és nem állami szervezetek egyaránt célozva, éppen ezért szükséges, hogy a különböző informatikai rendszerek mellett a felhasználók biztonságtudatosságát is fejlesszük. A kibertámadások alatt az információs dimenzióban megvalósuló hálózati hadviselést, vagyis a kibertérben bekövetkező műveletek összességét értjük. A kiberhadviselés célja a kiberfőlény kivívása és fenntartása, egyrészt a saját oldali – elektronikus, hálózatalapú információszerző, információtovábbító, és -feldolgozó – rendszerek védelmével, másrészt pedig a szembenálló fél hasonló rendszerei működésének zavarásával, korlátozásával, vagy akár elektronikus úton történő megsemmisítésével.¹ Számos korábban megtörtént eset bizonyítja, mekkora kárt, illetve veszélyt képes okozni a megfelelő védelem hiánya. Meggyőződésem szerint ezekből az esetekből nem csak tanulhatunk, de egyfajta iránymutatást is adhatnak, hogy hogyan cselekedjünk, illetve hogyan ne.

Megítélésem szerint a téma aktualitása miatt kiemelkedő jelentőséggel bír, éppen ezért szükséges a mélyebb vizsgálata, hiszen kellő felkészüléssel, az emberek biztonságtudatos viselkedésével az ilyen esetek bekövetkezése jelentősen csökkenthető.

A biztonságtudatosság nélkülözhetetlen eleme életünknek, mivel információs társadalomban élünk. Ez azt jelenti, hogy napjainkban az információ meghatározó társadalmi értéké válik, és a társadalom, illetve a gazdaság maga is információs értékeket termel és használ fel. Az információ előállítása, elosztása, terjesztése, használata-, és kezelése jelentős gazdasági, politikai és kulturális tevékenység egyaránt. Az információs társadalom működésének alapja az információs infrastruktúra (információs közműhálózat)². A számítástechnikai és elektronikai eszközök tárháza szinte végtelen. Az idő előrehaladtával folyamatosan jelennek meg új és új eszközök, amelyek számos veszélyt rejthetnek magukban. Éppen ezért szükséges, hogy mindennapjaink során megvédjük az információinkat a jogtalan hozzáféréstől, illetve az információk esetleges kiszivárgásától vagy megsemmisítésétől. A hatékony és eredményes védelem kialakítása érdekében biztosítani kell az adatok sértetlenségét, bizalmasságát és rendelkezésre állását. A bizalmasság alapján az információt csak az arra jogosultak és csak a jogosultságuk szintje szerint használhatják fel, illetve rendelkezhetnek a felhasználásról. A sértetlenség az információk és a feldolgozási módszerek teljességének és pontosságának megőrzését és az illetéktelen módosítások kizárását foglalja

¹ HAIG Zsolt, VÁRHEGYI István: A cybertér és a cyberhadviselés értelmezése. pp. 6-7. http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf, (Letöltés ideje: 2017. 11. 08.)

² HAIG Zsolt: Információ – társadalom – biztonság, Budapest, 2015, NKE Szolgáltató Kft., ISBN: 9786155527081, pp. 29-39.

magában. A rendelkezésre állás szerint az információknak kellő időben, illetve helyen, a jogosultak számára elérhetőnek és felhasználhatónak kell lennie, valamint elvesztésük, megsemmisülésük valószínűségét minimalizálni kell.³ Kizárólag ezen feltételek együttes teljesülése esetén beszélhetünk az információ megfelelő és hatékony védelmi mechanizmusáról. A védelem sikeres kialakítása érdekében, úgy gondolom fontos, hogy tudatosítsuk embertársainkban, milyen veszélyek várhatnak ránk, és ezeket miként tudjuk megelőzni, illetve milyen módon kell reagálnunk a már bekövetkezett eseményekre. Évről-évre bebizonyosodik számunkra, milyen sebezhetőek is vagyunk valójában, és hogy a védelem hiánya milyen beláthatatlan következményekkel járhat. A téma aktualitását tehát mi sem mutatja jobban, mint hogy naponta követnek el kibertámadásokat a különféle bizalmas és védendő információk megszerzése érdekében, éppen ezért elengedhetlen a biztonság tudatosság fejlesztése, hiszen ezáltal jelentősen csökkenthetjük a támadások bekövetkezésének valószínűségét.

Már az emberi civilizáció kezdete óta jelen voltak, illetve vannak az életünkben olyan fenyegetések, amelyekkel szemben szükség volt és van az információk védelmére. Már az ókorban és a középkorban is használtak különböző titkosításokat, kódolásokat⁴, amelyek a védelmet szolgálták. Az idő elteltével és a technika fejlődésével együtt nemcsak a különböző megtévesztési és behatolási technikák, de ezzel együtt a védelmi módszerek is egyaránt fejlődtek. Nem szabad elfelejteni azonban, hogy a támadók újabb és újabb módszereket alkalmaznak, ezáltal sok esetben a védekezés csak a támadást követő reakcióként jelenik meg. Napjainkra a klasszikus információs és kommunikációs rendszerek ellen vívott fegyveres küzdelem részévé vált a fizikális és digitális támadás. Azon tevékenységeket, amelyek a hálózatokba kapcsolt létfontosságú közintézmények, vagy egyéb, kormányzati szempontból jelentős eszközök és adatbázisok ellen irányuló cselekményt valósítanak meg, és amelyet valamely fegyveres konfliktus támogatására használnak, azokat a fegyveres műveletek részeként kell értelmezni. A támadásokat végrehajtó „digitális elkövetők” céljukat tekintve lehetnek például katonák, vagy akár terroristák is.⁵ Mint ahogy korábban említettem, a kibertámadások elsődleges célja a kiberfőlény megszerzése, azt azonban fontos kiemelni, hogy ezen támadások közvetett és közvetlen hatásokat egyaránt előidézhetnek. Ez alapján a kibertámadások egyrészt a fizikai rendszerek pusztítását, illetve katonai értelemben az ellenséges célpontok fizikai megsemmisítését eredményezik, másrészt a társadalom, a gazdaság, az oktatás, az egészségügy vagy akár a közszolgáltatás egyes elemeire is jelentős hatással vannak.⁶

³ 2013. évi L. tv Az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. § (1) bekezdés

⁴ Például a Julius Ceasar féle helyettesítéses titkosítás, amelynek során az abc-t három vagy 7 karakterrel eltolt abc-vel helyettesítette, és így írta le a szöveget.

⁵ SIMON László: Az információ mint fegyver? Szakmai Szemle 2016/1. p. 44. http://archiv.nbi.uni-nke.hu/uploads/media_items/simon-laszlo-az-informacio-mint-fegyver-szakmai-szemle-2016.original.pdf (Letöltés ideje: 2017. 11. 09.)

⁶ MAGYAR Sándor – SIMON László: A terrorizmus és indirekt hatása a kibertérben. Nemzetbiztonsági Szemle 2017/3. p. 97. http://archiv.uni-nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2017-3-1.original.pdf (Letöltés ideje: 2017. 11. 09.)

Megítélésem szerint a felhasználók nem elég biztonság tudatosak, lehet, hogy ismerik az őket érintő lehetséges veszélyeket, illetve fenyegetéseket, ennek ellenére nem hiszik, hogy ez velük is megtörténhet, így nem törődnek a különféle veszélyforrásokkal, illetve azok következményeivel. Éppen ezért úgy gondolom, már most fel kell készülnünk az ilyen lehetséges veszélyekre, ezért célom, hogy rávilágítsak az esetleges hiányosságokra és arra, hogy mennyire nélkülözhetetlen eleme mindennapjainknak a biztonság tudatosság kialakítása, illetve fejlesztése. A biztonság tudatosság kialakításának, illetve fejlesztésének első lépése a különféle „támadási alternatívák” ismerete, amely segítségével egy esetleges támadás bekövetkezése esetén felkészültek lehetünk.

A social engineering

Az információ biztonság területén a különféle bizalmas, illetve az adott szervezet belső működésével kapcsolatos információk megszerzésének egy jellemző típusa a social engineering.

A social engineering az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését. Douglas P. Twitchell egyetemi professzor szerint a social engineering a csalásnak vagy rábeszélésnek a gyakorlati alkalmazása bizonyos információk vagy ingóságok megszerzése érdekében.⁷

Kevin D. Mitnick az egyik leghíresebb hacker, a social engineering nagymestere „A legendás hacker” című könyvében így határozza meg a social engineering fogalmát:

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”⁸

Felmerül a kérdés, hogy napjainkban, amikor már a technológia robbanásszerűen fejlődik, és naponta jelennek meg új és új fejlesztések, eszközök, akkor mégis miért éppen egy állandóan változó, kiszámíthatatlan tényező áll a social engineering középpontjában? A humán tényező fontossága abban rejlik, hogy ez a tényező az, amely leginkább hatással van a legtöbb védendő értékre (információk, alkalmazások, informatikai infrastruktúra, emberi erőforrás).⁹ Az emberi tényező az adatokkal, információkkal kapcsolatban áll a létrehozásuk, megjelenítésük, módosításuk vagy esetleges törlésük, megsemmisítésük érdekében. Ahhoz, hogy az alkalmazott az adatokat fel tudja dolgozni, különböző szoftveralkalmazások, programok használatára jogosult. A szoftverek futtatásához szükség van megfelelő

⁷ TWITCHELL, Douglas P.: "Social Engineering and Its Countermeasures" Handbook of Research on Social and Organizational Liabilities in Information Security, pp. 228-242.

⁸ MITNICK, Kevin D.: A legendás hacker. A megtévesztés művészete, borító.

⁹ FLORES, Waldo Rocha, EKSTEDT Mathias: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, In. Computers and Security. pp. 26-44.

hardvereszközökre, az összeköttetéshez pedig a megfelelő belső hálózatra, így a humán tényező a hardvereszközök és adattárolók kezelése érdekében ismételtlen hozzáfér az informatikai infrastruktúrához, mint védendő értékhez.

Összességében tehát elmondható, hogy a humán faktor kritikus tényezőnek tekinthető, hiszen a tevékenysége kiterjed a szoftverek és hardverek használatára, hozzáférési jogosultsággal rendelkezik, számos adatbázis elérhető számára és a különböző belső információk birtokában van. Nem csak emiatt tekinthető kedvező célpontnak a felhasználó, hanem az embernek különféle kihasználható tulajdonságai is vannak. Ezek közé tartozik például a felhasználók hiszékenysége, naivsága, segítőkészsége, monotonitása, figyelmetlensége, befolyásolhatósága, illetve a szakértelem vagy a biztonságtudatosság hiánya is.

Ahhoz, hogy egy social engineering támadás ellen felkészültek legyünk és a megfelelő védelmet tudjuk biztosítani, mindenféleképpen ismernünk kell az adott támadási módszereket, technikákat. Fontos, hogy elhatároljuk a humán, vagyis az emberi megtévesztésen, befolyásoláson alapuló technikákat és az IT, vagyis az informatikai eszközök segítségével cselekvő módszereket.¹⁰

A humán alapú social engineering technikák esetében a támadó alapvetően nem a technológiai sérülékenységeket használja ki, hanem elsősorban a felhasználó különböző tulajdonságait használja a megtévesztésre. Ez ellen a módszer ellen nagyon nehéz védekezni, hiszen a támadó éppen a korábban említett tulajdonságainkat használja ki, azonban ebben az esetben a támadónak is nehezebb dolga van, hiszen a támadást személyesen, szemtől-szemben kell végrehajtania, ezáltal pedig a lebukás veszélye is sokkal nagyobb. A humán alapú social engineering technikák közé sorolható a segítségkérés¹¹ módszere, mely során a támadó egyszerűen csak megkérdezi az információt az adott alkalmazottól, vagy éppen segítséget kér tőle. A segítségkérés technikája kedvezőnek tekinthető a támadó számára, ugyanis az alkalmazottak sok esetben jóhiszeműek és naivak, nem gondolják, hogy az információ iránti igény egy támadás részét képezheti.

A következő technika a segítség nyújtása, vagyis a „fordított social engineering”, mely során a támadó kihasználja, hogy éppen egy problémával küszködünk, segítségre szorulunk, ezért az alkalmazott a támadó segítségét kéri, akinek már nem kell bebizonyítania hitelességét, szimplán csak meg kell oldania a felmerült problémát.¹²

Az identitáslopás technikája során a támadó egy másik személy bőrébe bújik, ezzel tévesztve meg az alkalmazottat. A megszemélyesítés célpontja lehet a szervezet alkalmazottja, például egy másik részleg munkatársa, vezetője, új kolléga,

¹⁰ DEÁK Veronika: A social engineering humán alapú támadási technikái. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (Letöltés ideje: 2017. 11. 09.)

¹¹ OROSZI Eszter: Social Engineering, http://kraszny.hu/presentation/diploma_oroszi.pdf pp. 31-33., (Letöltés ideje: 2017.07.04.)

¹² MITNICK 2003, i.m. pp. 55-75.

vagy akár a rendszergazda/IT szakember is, de a támadó egy takarító, karbantartó, vagy futár bőrébe is bújhat.¹³

A humán alapú technikák közé sorolható a jelszavak kitalálása is. A jelszavak egy részét valamilyen informatikai szoftver segítségével szerzik meg, míg másik részüket pedig az emberi figyelmetlenség, illetve hanyagság segítségével találják ki. Ezekre tökéletes példa az alapértelmezett jelszavak használata, a túl egyszerű jelszavak (0000, 1234, password, qwerty), az áldozat személyéhez kötődő jelszavak (születési dátum, becenév, családtagok neve), vagy akár a túl bonyolult jelszavak használata, hiszen ezek egy része könnyen kitalálható, másik részüket pedig a gyanútlan felhasználók sok esetben feljegyzik, amely megtalálása esetén a bizalmas információk könnyen illetéktelen kezekbe kerülhetnek.¹⁴

A „bejutás az épületbe”-módszer kiemelten fontos biztonságtechnikai szempontból is, hiszen ilyenkor a támadó észrevétlenül, a különféle beléptető rendszerek kikerülésével jut be az épületbe. A bejutás történhet a „tailgating”, vagyis a szoros követés technikájával, mely során a támadó a bejutáskor egy csoporthoz kapcsolódik szorosan, és úgy tesz, mintha annak tagja lenne. De történhet hamis belépőkártya használatával, vagy más jogosultságának a felhasználásával (piggybacking) is, amikor a támadónak nincs belépési jogosultsága az adott helyre, ezért kiadja magát egy másik személynek, akinek van, és jogosultságát felhasználva jut be a szervezet épületébe.¹⁵

További humán alapú social engineering technikának tekinthető a „dumpster diving”, vagyis a kukabúvárkodás. A technika lényege a kuka átvizsgálásában rejlik, mely során a támadó számos értékes információt tudhat meg rólunk, illetve munkahelyünkről az irodai vagy otthoni szemetesünk átvizsgálásával.¹⁶

A „shoulder surfing”¹⁷, vagyis a „vállszörfölés” technikája jelszavak vagy PIN kódok megszerzésére alkalmas, hiszen a módszer során a támadó kifigyeli, ahogyan a célszemély begépezi a jelszavát vagy a PIN kódját.

A social engineering technikák másik válfaja az IT, vagyis az informatikai eszközök segítségével cselekvő módszerek, amikor a támadó valamilyen informatikai eszköz segítségével próbálja megtéveszteni és átvenni az alkalmazottat. Ez különösen kedvező a támadónak, hiszen nincs személyes kontaktus, ezáltal a lebukás veszélye is sokkal kisebb. Ezen módszerek esetében a social engineer azt hiteti el az áldozatokkal, hogy egy valódi rendszerrel kommunikálnak, ezáltal pedig nem veszik észre, hogy valójában egy csalás áldozataivá válnak.

¹³ SÖRÖS Tamás et al.: Social engineering a biztonságtechnika tükrében, 2013, p. 9. http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orzagos.pdf (Letöltés ideje: 2017. 07. 12.)

¹⁴ Uo. p. 14.

¹⁵ Uo. pp. 15-16.

¹⁶ OROSZI 2008, i.m. pp. 37-38.

¹⁷ Uo. p. 38.

Az IT-alapú technikák egy jellemző válfaja az adathalászat, más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben, vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kéri a célszemélyt, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. Ez történhet például telefonos megkeresés, sms, e-mail, vagy akár hamis weboldal által.¹⁸

A kártékony programok csoportjába tartozó támadási technikák szintén bizonyos információk megszerzésére (jelszavak, szervezet belső információi, bankkártyaadatok) irányulnak, általában egy szoftver segítségével. Ez történhet például a frissítés, javítás felajánlásának módszerével¹⁹, mely során a támadó a gyártó nevében egy ingyenes frissítési vagy javítási lehetőséget ajánl fel, amelynek letöltése valamilyen kárt okoz. A kártékony programok csoportjába sorolhatók a keyloggerek, amelyek olyan billentyűzetleütés-naplózásra alkalmas programok, amelyek a felhasználó által begépelte karaktereket, illetve a képernyő tartalmát naplózzák, majd eltárolják azt. Később ehhez hozzáférhetnek, de akár tovább is küldhetik a támadónak, aki a naplózott karakterekből könnyen bizalmas információkhoz, például jelszavakhoz is juthat.²⁰

Továbbá ebbe a csoportba sorolhatók még a veszélyes csatolmányok. Ebben az esetben a támadó arra kéri a felhasználót, hogy nyissa meg a csatolmányt, mert az valamilyen fontos dokumentumot, képet tartalmaz, amit mindenféleképpen látnia kell, és azzal, hogy a felhasználó megnyitja azt, a kártékony program már aktiválódik is. Ez lehet akár vírus, programféreg, kémprogram, zsaroló program illetve trójai program is, amelyek látszólag, vagy akár valójában is hasznos funkciókat látnak el, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak, könyvtárakat, vagy akár adatállományokat törölnek.²¹

A vezeték nélküli internet kiemelten fontos, mivel jelentősen megkönnyíti mindennapjainkat. A kényelmesebb használat és számos más előnye mellett azért az egyik legfontosabb hátrányát mindenféleképpen meg kell említeni. A nyílt hozzáférésű WiFi-hálózatok különösen nagy veszélyt jelentenek számunkra, hiszen mi, mint felhasználók, nem tudjuk mennyire biztonságos az.²² Ha például egy közösségi helyen (kávézó, pláza, étterem), ahol sokan használják a WiFi-t, a támadó létrehoz egy nagy jelerősségű csatlakozási pontot, a gyanútlan felhasználó pedig ehhez kapcsolódik, nem is sejtve, hogy ezáltal a támadók megfigyelik a tevékenységét. Az is további kockázatot jelenthet, hogy ha egy gyengén védett hálózathoz hozzáférnek a támadók, hiszen sok esetben mi megbízunk például a

¹⁸ MUHA Lajos, KRASZNAY Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, 2014., NKE Szolgáltató Kft, p. 51. <http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9975/Teljes%20sz%c3%b6veg%21?sequence=1&isAllowed=y> (Letöltés ideje: 2017. 07.12.)

¹⁹ SÖRÖS et al. i. m. pp. 19-20.

²⁰ OROSZI 2008, i. m. pp. 52-54.

²¹ HAIG 2015, i. m. p. 131.

²² SÖRÖS et al. i. m. p. 24.

törzskávézónk WiFi-jében, de annak gyenge védettségét a támadók könnyen kihasználják, így jutva bizalmas információkhoz.

Az okostelefonjaink már mindennapjaink részévé váltak, azt azonban elfelejtjük, hogy nem árt óvatosnak lennünk, mivel minden alkalmazás hozzáfér a telefonunk tartalmához, az azonban nem mindegy, hogy mennyihez. „*Nem árt tudni, hogy vannak olyan rosszindulatú alkalmazások, amelyek távolról képesek a kamerát – ezáltal a mikrofont is – bekapcsolni és rögzíteni az eseményeket*”²³. A különböző letölthető alkalmazások – sokszor olyanok is, amelyek alapértelmezett alkalmazások, tehát alaphoz telepítve vannak a telefonjainkra – a használatukért cserébe számtalan olyan adathoz férnek hozzá, amely bizalmas számunkra és akár még zsarolás tárgyává is válhatnak. Ilyen információk például a tartózkodási hely, a névjegyek, az üzenetek (SMS, e-mail), a hívásadatok (tartalma, hossza), a képek, a videók, a kamera, az SD kártya tartalma, a telefonmemória tartalma, a hálózati hozzáférés, illetve a WiFi csatlakozási információk.

A következő IT-alapú technika adta a kutatásom alapját. A „baiting” magyarul odacsalogatást jelent, különféle csalikkal, amikor is valamilyen adathordozót (pendrive, CD, DVD) „véletlenül” szétszórtnak, elhagynak.²⁴ Amikor a gyanútlan felhasználó csatlakoztatja a számítógépéhez az eszközt, hogy kiderítse, kié lehet, vagy mi található rajta, már települ is a kártékony program, meg is fertőződött az eszköz, a program pedig segít megszerezni a bizalmas információkat, amelyekkel később könnyen visszaélhet a támadó, illetve meg is zsarolhatja az áldozatot.

Fontos kiemelni, annak ellenére, hogy számtalan social engineering technika létezik, a támadás sikeres véghezviteléhez az alábbi négy lépés szükséges²⁵:

1. az információszerzés,
2. a kapcsolat kiépítése,
3. a kapcsolat kihasználása,
4. a támadás végrehajtása.

A támadási módszertől függetlenül az első és legfontosabb lépés minden esetben a megfelelő információk megszerzése, összegyűjtése. Ez a fázis alapos munkát igényel, az alkalmazott módszertől függően hosszabb ideig, akár hetekig, hónapokig is eltarthat. A népszerűbb közösségi oldalak kitűnő kiindulási pontot jelenthetnek, hiszen a támadó a kiszemelt áldozatról számos személyes információt begyűjthet.²⁶ A támadó nem csak az elérhetőségeit (e-mail cím, esetleg telefonszám, lakhely), hanem számos egyéb információt is megszerezhet (érdeklődési kör, születési dátum, családi jellemzők), amelyek tökéletes alapot nyújthatnak például a jelszavak kitalálásához.

A megfelelő információk megszerzése után az áldozat kiválasztása és a vele való kapcsolat kiépítése következik, abban az esetben, ha az információszerzés

²³ MAGYAR – MOLNÁR p. 95.

²⁴ MUHA et al. i. m. p. 52.

²⁵ LEITOLD Ferenc: Sebezhetőségvizsgálatok a gyakorlatban, NKE Szolgáltató Kft., Budapest, 2014., pp. 11-12. <http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10450/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y> (Letöltés ideje: 2017. 07. 11.)

²⁶ Uo. p. 12.

fázisában már sikerült a támadónak megszereznie a céljaul kitűzött információt (például jelszót), akkor már a kapcsolat kiépítésére nincs szükség. A kapcsolatfelvétel történhet telefonon, e-mailben, közösségi portálon, de még akár személyesen is.²⁷

Miután a támadó megszerezte a szükséges információkat, kiválasztotta a megfelelő személyt és kialakított vele egyfajta bizalmi kapcsolatot, ezt követi a kapcsolat kihasználása. Ebben a fázisban a támadó segítséget kérhet az áldozattól, és előfordul, hogy már ilyenkor eléri célját, és megszerzi a számára szükséges bizalmas információkat, de sok esetben csak még tovább építi a bizalmat és egyre közelebb kerül a következő lépéshez, a támadás végrehajtásához.

Ha a támadónak az előző pontokban még nem sikerült elérnie célját, akkor a megszerzett információk, eszközök birtokában hajtja végre a már megtervezett támadást, károkozást. Ebben a fázisban kerül sor a felhasználó zsarolására, becsapására, vagy ha például a támadó megszerezte az áldozat jelszavát, akkor a végrehajtás fázisában kerül sor az adott rendszerbe való bejutásra és az ott tárolt adatok módosítására, felhasználására vagy esetleg törlésére.

A mai modern világunkban a különböző informatikai eszközök védelme már nagyon fejlett, így a támadó, ha például nem talál sebezhetőséget a felsőbb szinteken, mindig egy szinttel lejjebb megy, és addig csinálja ezt, amíg nem talál egy olyan pontot, ami sebezhető.

A védelem kialakításának első lépése, hogy felmérjük a jelenlegi helyzetet, feltérképezzük a sebezhetőségeket, hiszen a különböző óvintézkedések bevezetéséhez mindenképpen szükséges meghatározni azokat a területeket, amelyek különféle veszélyeket jelenthetnek. Fontos az alkalmazott eljárások folyamatos ellenőrzése és felülvizsgálata, illetve az emberek okozta sebezhetőségek feltérképezése egy általános információbiztonsági audit, sérülékenységvizsgálat vagy akár egy betörésteszt segítségével.²⁸

Ha feltártuk a hiányosságokat, a vizsgálatok eredményétől függően, megkezdődhet a probléma orvoslása, ennek keretében a biztonsági előírások kidolgozása, a jelenleg alkalmazott szabályok esetleges módosítása, illetve az esetleges hiányosságok pótlása. Napjainkban már minden szervezet rendelkezik valamilyen biztonsági szabályzattal; ahány szervezet, annyi típussal találkozhatunk. Számos olyan előírás van, amely az információbiztonsági politikába való beépítésével és az alkalmazottakkal való ismertetésével, a social engineering támadások bekövetkezésének valószínűsége csökkenthető. Fontos, hogy ezeket a szabályokat, ne csak elkészítse az adott szervezet, hanem kiemelt figyelmet fordítson azok betartására is. Az esetleges biztonsági előírásnak tekinthetők például a fizikai biztonságra, a különféle informatikai eszközökre, a hordozható és leselejtezett eszközökre, a hulladékkezelésre, az iratmegsemmisítésre vonatkozó, az elektronikus levelezésre, valamint a felhasználók oktatásával és a telefonhívásokkal kapcsolatos előírások.

²⁷ OROSZI 2008, i. m. p. 59.

²⁸ OROSZI 2008, i. m. p. 62.

A következő, és egyben az egyik legfontosabb lépés a felhasználók biztonságtudatossági oktatása és az aktuális előírások ismertetése.

Biztonságtudatossági kísérlet

A biztonságtudatosság fontosságának ábrázolását egy egyetemi hallgatói környezetben végzett biztonságtudatossági kísérlet segítségével terveztem bemutatni. A hallgatók biztonságtudatosságát vizsgáltam egy social engineering támadással, valamint ezt követően kérdőíves kutatást végeztem a kísérletben résztvevők körében.

A kísérlet célja az volt, hogy felmérjem a hallgatók biztonságtudatosságát és rávilágítsak az esetleges hiányosságokra, amelyek a biztonságtudatosság megfelelő fejlesztésével bizonyos mértékben orvosolhatók. Ez kiemelten fontos, mivel a biztonságtudatosság megfelelő szintjével az esetleg támadások bekövetkezésének valószínűsége csökkenthető.

A kísérlettel azt vizsgáltam, hogy telefont használó fiatalok mekkora hányada csatlakoztatja okostelefonját egy idegen, számukra ismeretlen eszközhöz. A kísérletben a social engineering egyes módszereit alkalmaztam. A célcsoport tagjainál a „közreműködő megtevesztésnek” a célja az volt, hogy az önkéntes résztvevők minél több hiányossággal szembesüljenek. A kísérlethez engedélyt kértem és kaptam a Kar vezetésétől. A doboz valójában kizárólag ártalmatlan ál-csatlakozókat tartalmazott, így a remélt csatlakozást követően a mobiltelefonokkal semmilyen kapcsolat nem jött létre. Semmi nem töltődött fel vagy le, a hallgatók eszközeit semmi nem veszélyeztette.

A kísérlet fő eszköze egy telefontöltőnek látszó fa doboz volt, amely azt a látszatot keltette, hogy az az egyetem nyílt szolgáltatása a telefonok szabad feltöltésére. Az eszköznek nem csupán a funkcióját, tulajdonságait, hanem az elkészítését is részletesen ismertetem, mert minden apró részlet kulcsfontosságú volt a doboz külső megítélése miatt. A megfelelő megítélés pedig azért volt fontos, hogy minél többen csatlakozzanak az ál-készülékhez – ezzel a felméréshez is – és egyben bizonyítsam a social engineering hatásosságát.

A doboz tulajdonságai közül a látványa a meghatározó, mivel mind funkciójának, mind a tulajdonságainak nagy részét ebből mérheti fel az érdeklődő. Nagyon fontos, hogy az az idő, ami rendelkezésemre állt, cselekvésre motiváljon, ez megközelítőleg pár másodperc volt. Ennyi idő alatt kellett a doboznak a hallgató érdeklődését felkelteni, a doboz funkcióját tudatosítani, és a bizalmának alapját megteremteni.

Az eszköz funkciói:

- az érdeklődés felkeltése,
- a hallgató számára hasznos funkció felismertetése,
- a bizalomkeltés,
- a kísérlet mérése (amelyet az eszközön végeztem, a csatlakoztatás tényének megállapításával, illetve az interjúk elkészítésével).

A látványelemek legtöbbje így a fenti célokat szolgálja. Az érdeklődés gyors felkeltését az eszköz elhelyezése egy kifejezetten forgalmas helyen, a kiálló és jól felismerhető csatlakozók, illetve a látványos lakat szolgálta. A doboz funkciójának bemutatását a „Telefontöltő” felirat és a kiálló csatlakozók „végezték”. A bizalmat – első pillantásra – az egyetem logója, a doboz ízléses megjelenése és a lakat hivatott megalapozni. A bizalmat (tovább) erősíteni már a technikai tulajdonságoknak kellett, amelyek egyben arra is szolgáltak, hogy minél több hallgatót vonjanak be a kísérletbe. Igyekeztem mindenki számára biztosítani a lehetőséget, hogy a felmérés hatékonyabb legyen és minél realisabb eredményeket tükrözzön.

Megjegyzem, annak érdekében, hogy a megmunkálás és a kialakítás sokkal precízebb legyen, szülői segítséget vettem igénybe. Egy általam összebarkácsolt fa dobozról nem hitték volna el a hallgatók, hogy azt az egyetem készítette, és hogy megbízhatóan működik.

Ezek után belátható, hogy már az előkészítés első lépése, a feladatra alkalmas doboznak a beszerzése sem volt egyszerű feladat. Végül egy kreatív célokra felhasználható fadobozt sikerült vásárolnom, ami megfelelő alapot jelentett a követelmények teljesítéséhez. A doboz kialakításánál nyitott doboz nem jöhetett szóba, hiszen akkor a hallgatók – belelátva – rájöhettek volna, hogy ez valójában nem egy töltő, hanem csak egy kísérlet, amelynek keretében különböző – nem működő – töltőket helyeztem be egy fa dobozba. Ugyanakkor biztosítani kellett, hogy a készülék összeszerelhető legyen, és keltse is azt a látszatot, hogy szervizelhető. A doboz lezárását lakattal terveztem, a lakat felkerülését követően pedig lefestettem a dobozt, hogy ezáltal is növeljem a hitet a hallgatókban, hogy az eszköz az egyetem tulajdona. Végül az egyetem logóját és a „Telefontöltő” feliratot, kinyomtattam és ráragasztottam a doboz tetejére, hogy amikor valaki elsétál a doboz mellett, vagy csak rápillant, rögtön ezeket az információkat kapja meg. Hiszen ezek a legfőbb üzenetek, az embléma pedig azt a látszatot kelti, hogy ez az egyetem tulajdona, ezáltal pedig bizalmat közvetít a hallgatók felé, bizalmat kelt és azt a hamis érzetet, hogy nem fenyegeti semmi veszély, ha rácsatlakozik. Ez különösen fontos volt, hiszen, ha a hallgatók nem tartanak a fenyegetéstől, akkor rá fognak csatlakozni az eszközre. A dobozt végül kétoldalú ragasztó segítségével az asztalhoz rögzítettem, amellyel megteremttem a fizikai stabilitását, még inkább azt bizonyítva a hallgató számára, hogy ez nem ideiglenes dolog, hanem az egyetem stabil szolgáltatása.

Az álcsatlakozók kialakításánál elsődleges szempont volt, hogy minél több telefont lehessen rácsatlakoztatni, más szóval minél kevesebbet korlátozzak ebben azzal, hogy nem talál kompatibilis csatlakozót a töltéshez. Ezért sok és többféle csatlakozó került a dobozba. A telefongyártók még ma sem használnak teljesen egységes töltőcsatlakozókat, még saját gyártmányaikon sem. A különböző csatlakozók felhasználásának célja az volt, hogy a hallgató készülékének portja passzoljon valamelyik csatlakozóhoz az eszközön. Egy okostelefon esetében ez lehet a ma már számos USB csatlakozó valamelyike (az újabbaknál micro-USB), de egyes készülékek esetében például 30 tűs csatlakozó, vagy lightning is. A választékot tovább bővítettem azzal, hogy beszereltem három hálózati csatlakozó aljzatot is, hogy ezáltal minden hallgató személyre szabottan, a saját telefonjához illeszkedő töltőt csatlakoztathasson hozzá.

Tehát a közepes és nagymértékben elterjedt csatlakozási lehetőségeket mind beépítettem, így a kísérletben a legtöbb telefontípust használó hallgató részt vehetett.

Ahhoz, hogy ezek a kábelek, illetve a hálózati tápegységek látsszanak is ki a dobozból, és rá is tudjanak kapcsolódni, ki kellett vágni a fa doboz oldalait.

A kísérlet ugyan a biztonságtudatosság-béli hiányosságok feltárását célozta, azonban számolnom kellett azokkal a hallgatókkal is, akik jobban vagy teljesen felkészültek a témában, így akár tüzetesebben is megvizsgálják a készüléket. A social engineering eszköztárában vannak módszerek az ilyen helyzetekre is. A látható hardver-elemek összeállítása mellett ezért külön figyelmet szenteltem az „álcázásra”. Arra törekedtem, hogy a készülék fizikai vizsgálata az ő bizalmukat is elnyerje. Ennek érdekében nem csupán lerögzítettem a dobozt egy duplaoldalas ragasztóval, de – egy esetleges elmozdítás esetére – félrevezetően alakítottam ki. A belsejét kitömtem, hogy a vizsgáló személyt – a súlyérzékelését felhasználva – arra a hamis következtetésre juttassam, hogy a doboz akkumulátort tartalmaz a töltéshez. Ezzel egyben a hallását is megcsaltam: a doboz belsejében a kitömés mindent még jobban rögzített, hogy akkor se legyen hallható zörgés, ha a hallgató megrázná a dobozt.



1. ábra: Az eszköz képeiben
(Saját szerkesztés)

Az eszköz kivitelezése azért kiemelten fontos, mert ahogyan én el tudtam készíteni ezt a dobozt, illetve mindenféle különleges azonosítás nélkül besétáltam az intézménybe és kihelyeztem az eszközt, úgy bárki más is megteheti ezt. A doboz kihelyezése mellett fontosnak tartottam, hogy akiből valamilyen reakciót vagy véleményt váltott ki a doboz látványa, mindenféleképpen megkérdezzem a saját álláspontjáról. Éppen ezért egy 7 (nappali tagozaton) és 8 (levelező tagozaton) kérdésből álló interjút készítettem velük. A különbség a két kérdéssor között az volt, hogy a levelezős hallgatók számára a hivatali levelezéssel kapcsolatosan is feltettem egy kérdést, ezzel szemben a nappali tagozatos hallgatók esetében azt vélelmeztem, hogy a hallgatók jelentős része nem dolgozik, ezért esetükben ettől a kérdéstől

eltekintettem. Az interjú azért kiemelt jelentőségű, mert a kísérlet csupán egy oldalról közelíti meg a hallgatók biztonság tudatosságát, a kérdőívvel azonban egyéb, a biztonság tudatossággal kapcsolatos szokásaikat is megvizsgálhattam. A kísérletet két alkalommal, egy levelező és egy nappali tagozatos tanítási napon végeztem. A levelező tagozatos hallgatók biztonság tudatosságát azért vizsgáltam, mert kíváncsi voltam, hogy egy másik korosztály hogyan reagál egy ilyen eszközre, illetve azért, hogy összehasonlítsam a nappali tagozatos hallgatók biztonság tudatosságával.

Levelező tagozatos hallgatók kísérlete

A levelezős hallgatók kísérletét egy szombati napon tartottam. Fontos szempont volt, hogy még a hallgatók megérkezése előtt kirakjam a dobozt, nehogy meglássák, hogy nem egy hivatalos személy teszi ki. A dobozt közvetlenül a büfé melletti asztalhoz helyeztem el, egyrészt mert ha a hallgatók vásárolnak valamit a büfében, akkor ahhoz közel foglalnak helyet, és ott fogyasztják el a vásároltakat, illetve a lépcsőhöz közeli oldalra tettem, abból a feltételezésből, hogy ott foglalnak alapvetően helyet, hiszen a lépcső és a lift közelsége miatt elég később is elindulniuk a szemináriumokra vagy előadásokra. Miután kivettem az eszközt, a kísérlet végéig kellő távolságból figyeltem a történeteket, és jegyzőkönyvbe vettem minden cselekvést, amely a dobozhoz köthető. Az interjú készítésekor megkértem a hallgatókat, hogy a kísérletről ne számoljanak be társaiknak, hogy ne korrumpálódjon az által, hogy egymás közt megbeszélnek.

Összesen tizenhárom hallgató nézte meg közelebbről az eszközt, 38,46%-uk (5 fő) használta konkrétan az eszközt, a többiek (61,54%) megnézték, azonban valamilyen okból kifolyólag mégsem használták. Annak magyarázata, hogy miért használták, illetve miért nem, igen különbözőek voltak. Volt olyan hallgató, aki azt mondta, hogy a jelenleg a világban zajló terrorfenyegetettségek hatására minden doboznak kinéző eszköztől automatikusan rossz érzés fogja el, és azonnal egy lehetséges terrortámadás bekövetkezésére asszociál. Egy másik hallgató azt mesélte, hogy a munkatársai meséltek neki arról, hogy mennyire elterjedtek az olyan eszközök, mint például a pendrive, amely által valamilyen vírussal akárják megfertőzni az illető számítógépét, így ebből kifolyólag ő a számítógépéhez sem csatlakoztat kétes eredetű eszközt, illetve a telefonjával sem kapcsolódik olyan tárgyhoz, amelynek eredetét nem ismeri. Az öt hallgató, akik rácsatlakoztatták okostelefonjukat az eszközre, azzal indokolták, hogy megbíztak a töltőben, hiszen az egyetem logója volt rajta, illetve volt olyan, aki azt mondta, hogy egyáltalán nem tart az esetleges USB-csatlakozókon fellepülő vírusoktól, vagy éppen az adatlopástól sem, egyszerűen csak szüksége volt töltőre, így attól függetlenül, hogy ez egy idegen eszköz, félelem nélkül használta azt. Három hallgató azt nyilatkozta, hogy mindenféle „technikai kütyütől” fél, így megnézték, de eszközbe sem jutott csatlakozni az eszközre. Két hallgató pedig azt nyilatkozta, hogy az egyetem milyen hallgatóbarát, illetve, hogy milyen jó ötlettel könnyítik meg a hallgatók életét, hiszen egész nap bent vannak, így sokszor szükségük van teleföntöltőre, ebben az esetben azonban csak azért nem használták, mert éppen nem volt szükségük rá, abban az esetben, ha a telefonjuk töltöttsége alacsony lett volna, mindenképpen feltöltötték volna. Arra a kérdésre, hogy miért, szintén azt válaszolták, hogy mivel az egyetem nevét viseli a töltő, ezért fel sem merült bennük, hogy ez esetleg veszélyes is lehet. Egy másik hallgató pedig azt válaszolta, hogy csak azért nem használta, mert mikor meglátta, már hazafelé tartott, így szükségtelen volt számára.

Az interjú első kérdése az volt, hogy milyen módszerrel védik eszközeiket a kártékony programok ellen. Ezt a kérdést azért tettem fel, hogy felmérjem, ismerik-e a különböző védelmi eszközöket, abban az esetben, ha nem, akkor iránymutatást adjak nekik a lehetséges módszerekről. Mindannyian azt a választ adták, hogy vírusirtókkal és/vagy tűzfalal védik, arról azonban arról, hogy milyen egyéb védelmi módszerek vannak, nem hallottak.

A következő kérdésre, hogy szoktak-e nyílt hozzáférésű WiFi-hálózatot használni, a válaszolók 23,08 %-a, tehát mindössze három hallgató válaszolt nemmel, a többiek (76,92) viszont gyakran csatlakoznak nyílt hozzáférésű WiFi-hálózatokhoz. A legtöbben azt mondták, hogy kávézóban, éttermekben, bevásárlóközpontban vagy a távolsági vonat-, illetve autóbuszjáratokon csatlakoznak ilyen hálózatokra. Ez azért lényeges, mert a nyílt hozzáférésű WiFi-hálózatok különösen nagy veszélyt jelentenek számunkra, hiszen mint már korábban említettem: például, ha a támadó egy közösségi helyen (étterem, kávézó) létrehoz egy nagy jelerősségű csatlakozási pontot, a gyanútlan felhasználó pedig ehhez kapcsolódik, nem is sejtve, hogy ezáltal a támadók megfigyelik a tevékenységét.

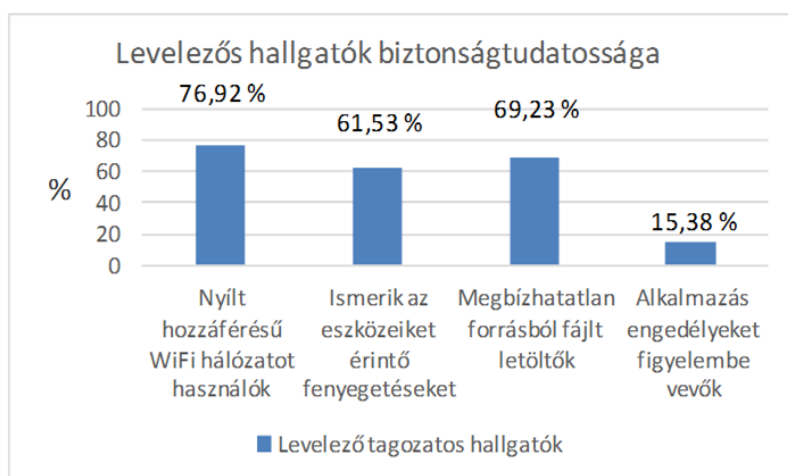
A harmadik kérdés a saját eszközeiket érintő fenyegetésekhez kapcsolódott. A hallgatók 61,53%-a válaszolta azt, hogy tisztában van az eszközeiket fenyegető veszélyekkel, és nagy részük a vírusokat, illetve az adathalászatot említette lehetséges veszélyforrásként. A válaszadók 38,47%-a pedig nem tudja, milyen kockázatokkal kell szembenézniük a telefonjaikat illetően. A kérdés fontossága abban rejlik, hogy ha a hallgatók nem ismerik a különböző fenyegetéseket, kockázatokot, akkor azt sem fogják tudni, hogy hogyan védekezzenek ellene. Ennek kapcsán lehetséges veszélyként a legtöbben a különböző vírusokat és az adathalászatot említették meg.

Arra a kérdésre, hogy szoktak-e megbízhatatlan forrásból fájlokat letölteni, a válaszadók 69,23%-a válaszolt igennel, és 30,77%-uk pedig nemmel. Amikor megkérdeztem az igennel válaszolókat, hogy miért töltenek le ilyen webhelyekről, azt felelték, hogy nem tudják, milyen veszélyt rejtenek ezek, és hogy nem tudják felismerni, hogy egy webhely biztonságosnak, vagy éppen megbízhatatlannak számít-e, ebben az esetben pedig könnyen kártékony programok áldozatává válhatnak.

A hatodik kérdés az alkalmazásengedélyekre vonatkozott. A hallgatók 84,62%-a válaszolta: lehet, hogy elolvassa, hogy a különböző alkalmazások milyen adataihoz férnek hozzá, azonban ettől függetlenül is letöltik azt, mert szükségük van rá. A válaszadók mindössze 15,38%-a (2 hallgató) veszi figyelembe egy alkalmazás letöltésénél, hogy az mely adataihoz fér hozzá. Ez azért kiemelkedő jelentőségű, mert, ha valaki ezekhez az információinkhoz hozzáfér, rögtön megjelenik a zsarolás lehetősége, amellyel könnyen rávehet minket a támadó egyéb bizalmas információk átadására is.

Az utolsó kérdés arra vonatkozott, hogy a hallgatók a hivatali rendszerből el szokták-e küldeni leveleiket a magán e-mail címükre, hogy ezáltal akár telefonról, akár tabletről egyszerűbben hozzáférhessenek. A hallgatók 30,77%-a nemmel válaszolt, 69,23%-a pedig igennel. Legtöbben azt felelték, azért küldik el, hogy így akár otthon, vagy akár utazás közben is tudják intézni a hivatali ügyeiket.

Az alábbi, 2. számú ábrán az interjú során feltett kérdések százalékos megnyilvánulásai láthatók.



2. ábra: A levelező tagozatos hallgatók biztonság tudatossága
(Saját szerkesztés)

Nappali tagozatos hallgatók kísérlete

A nappali tagozatos hallgatók kísérletét egy szerdai napon tartottam, ugyanis az előzetes megfigyeléseim azt bizonyították, hogy az öt tanítási napon szerdán tartózkodnak az egyetemen a legtöbben. Ez esetben is fontos szempont volt, hogy még a hallgatók megérkezése előtt kirakjam a dobozt, nehogy meglássák, hogy nem egy hivatalos személy teszi ki. A dobozt ebben az esetben is közvetlenül a büfé melletti asztalhoz helyeztem el, ugyanazon indokok miatt, mint a levelezős hallgatók esetében. Miután kivettem az eszközt, a kísérlet végéig egy másik asztaltól figyeltem a történeteket, és jegyzőkönyvbe vettem minden cselekvést, amely a dobozhoz köthető. A nappali tagozatos hallgatók kísérleténél még inkább értelmet nyert az eszköz kétoldalú ragasztóval történő rögzítése, ugyanis a kísérlet folyamán 6 hallgató próbálta meg elvinni az eszközt.

Összesen huszonhat hallgató nézte meg közelebbről az eszközt, 80,76%-uk (21 fő) használta konkrétan az eszközt, a többiek (19,23%) megnézték, azonban valamilyen okból kifolyólag mégsem használták. Annak magyarázata, hogy miért használták, illetve miért nem, igen különbözőek voltak. Volt olyan hallgató, aki azt mondta, hogy azért nem használta, mert kizárólag csak a saját töltőjével tölti a telefonját, idegen eszközökhöz semmiképpen nem csatlakoztatná telefonját. Egy másik hallgató azt mesélte, hogy nem bízott az eszközben, attól függetlenül, hogy az egyetem logója szerepelt a dobozon, nem látta még itt ezt az eszközt, ezért nem csatlakozott rá. Három hallgató azt mondta, hogy csak azért nem csatlakoztak az eszközre, mert nem volt lemerülve a telefonjuk, abban az esetben, ha az lett volna, mindenféleképpen használták volna.

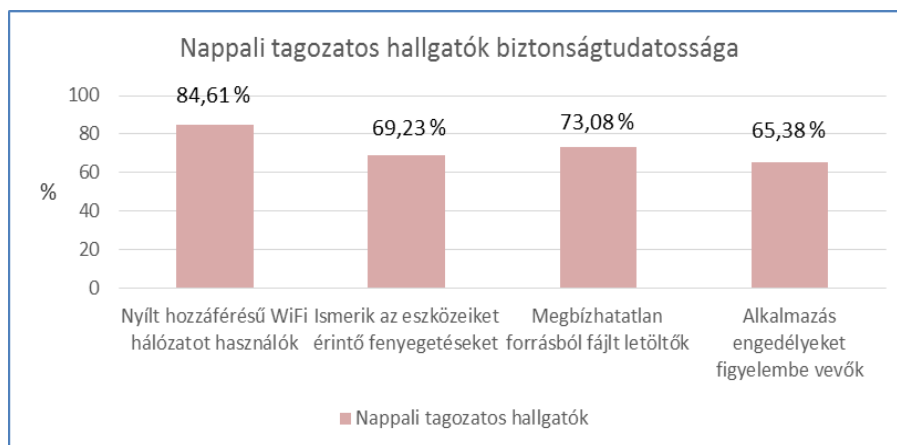
A huszonegy hallgató, akik rácsatlakoztatták okostelefonjukat az eszközre, többféle indokkal szolgáltak. Volt olyan hallgató, aki azt mondta, hogy nem működik a töltője, jelenleg egy másik márka töltőjével tölti, így kipróbálta, esetleg ezzel az eszközzel működik-e. Többen azt állították, hogy csak kíváncsiságból csatlakoztak rá a töltőre, jó ötletnek tartották, nem látták még itt ezt az eszközt, így kipróbálták, hogy működik-e. Összességében megállapítható, hogy a nappali hallgatók hasonló válaszokat adtak az eszköz használatát illetően, mint a levelezős hallgatók, ugyanúgy azt nyilatkozták, hogy bíznak az eszközben, nem féltek tőle, illetve szükségük volt telefonjuk feltöltésére, így bátran használták a kihelyezett töltőt.

Az interjú kérdéseire elég vegyes válaszok érkeztek, némelyeknél feltételezhető volt a biztonságtudatosság bizonyos foka, míg más kérdések esetében egyáltalán nem.

Az interjú első kérdése az volt, hogy milyen módszerrel védik eszközeiket a kártékony programok ellen. A válaszok igen különbözőek voltak. A legtöbben azt a választ adták, hogy vírusirtókkal és/vagy tűzfalal védik, arról azonban, hogy milyen egyéb védelmi módszerek vannak, nem hallottak. Mindössze két hallgató említette meg a hozzáférés-szabályozást, mint a védelem eszközét, ezen belül is a jelszavas védelmet.

A következő kérdésre, hogy szoktak-e nyílt hozzáférésű WiFi-hálózatot használni, a válaszolók 15,38 %-a, tehát mindössze négy hallgató válaszolt nemmel, a többiek (84,62%) viszont gyakran csatlakoznak nyílt hozzáférésű WiFi-hálózatokhoz. A legtöbben azt mondták, hogy kávézókban, cukrászdákban, éttermekben, bevásárlóközpontban vagy a távolsági vonat-, illetve autóbuszjáratokon csatlakoznak ilyen hálózatokra.

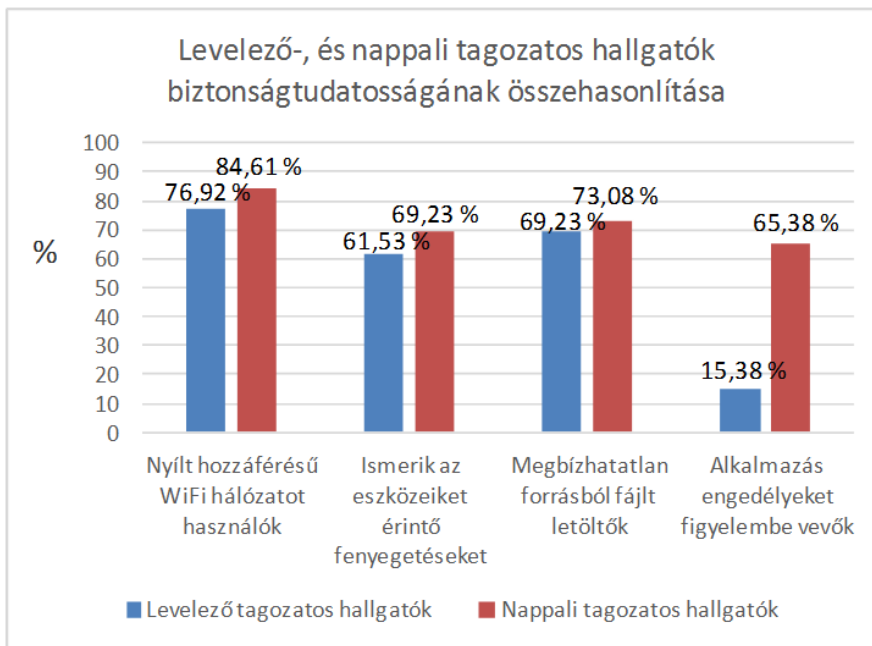
A harmadik kérdés a saját eszközüket érintő fenyegetésekhez kapcsolódott. A hallgatók 69,23% válaszolta azt, hogy tisztában van az eszközeiket fenyegető veszélyekről, és nagy részük a vírusokat, illetve az adathalászatot említette lehetséges veszélyforrásként. A válaszadók 30,77%-a pedig nem tudja, milyen kockázatokkal kell szembenézniük a telefonjaikat illetően. Ez azért jelent komoly problémát, mert ha a hallgatók nem ismerik a különböző fenyegetéseket, akkor azt sem fogják tudni, hogy hogyan védekezzenek ellene. Ennek kapcsán lehetséges veszélyként a nappali tagozatos hallgatók is a különböző vírusokat és az adathalászatot említették meg. Arra a kérdésre, hogy szoktak-e megbízhatatlan forrásból fájlokat letölteni, a válaszadók 73,08%-a válaszolt igennel, és 26,92%-uk pedig nemmel. Amikor megkérdeztem az igennel válaszolókat, hogy miért töltenek le ilyen webhelyekről, azt felelték, hogy nem tudják, milyen veszélyt rejtenek ezek, és hogy nem tudják felismerni, hogy egy webhely biztonságosnak, vagy éppen megbízhatatlannak számít-e. A hatodik kérdés az alkalmazásengedélyekre vonatkozott, melyek tekintetében a hallgatók 65,38%-a válaszolta, hogy elolvassák az egyes alkalmazások esetében, hogy mely adataikhoz férnek hozzá, és ezek fényében döntenek az adott alkalmazás letöltéséről. A válaszadók 34,62%-a azt nyilatkozta, hogy az alkalmazások letöltésénél nem veszik figyelembe, mely adataikhoz fér hozzá az adott alkalmazás. Az alábbi 3. számú ábrán az interjú során feltett kérdések százalékos megnyilvánulásai láthatók.



3. ábra: A nappali tagozatos hallgatók biztonságtudatossága
(Saját szerkesztés)

Összegezve, annak ellenére, hogy az esetszámokat tekintve nem minősül reprezentatívnak a vizsgálat, számos tanulság levonható. A levelező és nappali tagozatos hallgatók többsége azt nyilatkozta, hogy ismerik a saját eszközeiket érintő fenyegetéseket, ám ennek ellenére az interjú azt az eredményt mutatta, hogy lehet, hogy ismernek néhány kockázatot, ám ez kevés. Hiszen, ha nem ismerik a fenyegetések és kockázatok típusait, akkor a védekezés módszereit sem ismerhetik. Az alábbi 4. számú ábra tökéletesen mutatja a két kísérlet különbségeit. A levelezős hallgatók óvatosabbak voltak az eszköz használatát és a különböző egyéb veszélyes cselekményeket illetően is. Így például a levelező tagozatos hallgatók kisebb arányban használnak nyílt hozzáférésű hálózatokat és töltenek le megbízhatatlan forrásból különféle fájlokat, mint a nappali tagozatos hallgatók. Ám az alkalmazásengedélyekkel kapcsolatos kérdés elég szélsőséges eredményeket mutatott, ez esetben a nappali tagozatos hallgatók voltak a biztonság tudatosabbak, hiszen 65,38%-uk mondta azt, hogy egy alkalmazás letöltésénél figyelembe veszik, mely adataikhoz kér hozzáférést az adott alkalmazás, és ennek függvényében döntenek annak letöltéséről. Ezzel szemben a levelezős hallgatók mindössze 15,38%-a mondta azt, hogy ez szerepet játszik az alkalmazás letöltésekor.

Az eszköz használatával kapcsolatos tevékenységet és az interjúk során elhangzottakat egybevéve, a levelezős hallgatók bizonyultak biztonság tudatosabbnak, ám megítélésem szerint ez nem feltétlenül a kockázatok és az azokra irányuló védekezési módszerek ismeretének tudható be, hanem inkább az ismeretlentől való félelemnek, illetve az óvatosságnak.



4. ábra: A levelező és nappali tagozatos hallgatók biztonság tudatossága
(Saját szerkesztés)

Összegzés

Napjainkban már a kezelt információk fajtáinak száma, mennyisége sokszorosa a korábbiakénak, tárolásuk pedig igen nagy koncentrációban történik. Aki ezekhez hozzáfér, óriási erőforráshoz jut. A felhasználások céljai nem változtak alapjaikban, viszont tömegessé váltak a különféle információlopások és az illegális felhasználások is. Aggasztó, hogy már szinte mindenkinek lehetősége van az internetről beszerezni a megfelelő információt, és hogy a gazdasági szereplők és a társadalom egyre nagyobb része használja fel a megszerzett adatokat. Az információk kezelőinek így óriásira nőtt a felelőssége, különösen az állami szerveknél, ahol mind a gazdaság résztvevőiről, mind az állampolgárokról, mind az állami szervekről óriási mennyiségű információ összpontosul.

Ez teszi kulcsfontosságúvá a biztonság tudatos viselkedés szabályrendszerének kialakítását, megtanítását és betartatását – a legalsó pozíciótól a legfelső vezetői szintig. Az információbiztonsággal foglalkozó szakembereknek meg kell mutatniuk számukra, hogy mekkora kárt tud okozni, illetve mekkora veszélyt jelent az adatok megfelelő védelmének hiánya, mekkora felelősség terheli az egyes résztvevőket, és hogyan tudnak megfelelni a biztonsági elvárásoknak.

A különböző támadás módszereit megismerve és megismertetve jelentősen tudjuk csökkenteni a ránk bízott információk kiszivárgását és illetéktelen felhasználását, egyúttal az állami szervek működésének stabilitását, a társadalom és a gazdaság résztvevőinek biztonságát.

Felhasznált irodalom:

- DEÁK Veronika: A social engineering humán alapú támadási technikái. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (Letöltés ideje: 2017. 11. 09.)
- FLORES, Waldo Rocha; EKSTEDT, Mathias: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, In. Computers and Security. pp. 26-44.
- HAIG Zsolt: Információ – társadalom – biztonság., Budapest, 2015, NKE Szolgáltató Kft., ISBN: 9786155527081
- HAIG Zsolt, VÁRHEGYI István: A cybertér és a cyberhadviselés értelmezése. http://mhht.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf, (Letöltés ideje: 2017. 11. 08.)
- MAGYAR Sándor – SIMON László: A terrorizmus és indirekt hatása a kibertérben. Nemzetbiztonsági Szemle 2017/3. pp. 89-101. http://archiv.uni-nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2017-3-1.original.pdf (Letöltés ideje: 2017. 11. 09.)
- MAGYAR Sándor – MOLNÁR Péter: Vállalati mobiltelefonok védelmének lehetősége MDM megoldással. Szakmai Szemle, 2015/4., pp. 89-102
- LEITOLD Ferenc: Sebezhetőségvizsgálatok a gyakorlatban. NKE Szolgáltató Kft., Budapest, 2014. <http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10450/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y> (Letöltés ideje: 2017. 07. 11.)
- MITNICK, Kevin D.: legendás hacker. A megtévesztés művészete, Budapest, 2003., Perfact-Pro, ISBN: 9789632065557
- MUHA Lajos – KRASZNAY Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. Budapest, 2014., NKE Szolgáltató Kft, <http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9975/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y> (Letöltés ideje: 2017. 07. 12.)
- OROSZI Eszter: Social Engineering, 2008, http://kraszny.hu/presentation/diploma_oroszi.pdf (2017. 07. 04.)
- SIMON László: Az információ mint fegyver? Szakmai Szemle 2016/1. pp. 34-60. http://archiv.nbi.uni-nke.hu/uploads/media_items/simon-laszlo-az-informacio-mint-fegyver-szakmai-szemle-2016.original.pdf (A letöltés ideje: 2017. 11. 09.)
- SÖRÖS Tamás et al.: Social engineering a biztonságtechnika tükrében, 2013. http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orszagos.pdf (Letöltés ideje: 2017. 07. 12.)

- TWITCHELL, Douglas P.: "Social Engineering and Its Countermeasures" Handbook of Research on Social and Organizational Liabilities in Information Security, Kennesaw, Georgia, USA, 2006.
- 2013. évi L. tv Az állami és önkormányzati szervek elektronikus információbiztonságáról

KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA I.

Bevezetés

A tanulmány célja az elérhető nyílt források felhasználásával egy átfogó kép bemutatása a Koreai Népi Demokratikus Köztársaság² kiberstratégiájáról, a kibertevékenység szervezéséről és annak szervezeti kereteiről, valamint a hírhedt Lazarus csoport tevékenységéről. Az Észak-Koreával kapcsolatos elérhető információforrások köre nagyon szűkös. Nehéz megbízható forrásból származó, ellenőrzött információt szerezni az ország belső életéről, különösen igaz ez a katonai, vagy titkosszolgálati vonatkozású információkra, ezért a nemzetközileg elismert hírszolgálatok tudósításain túl a tanulmány elkészítésénél nagymértékben támaszkodtam a washingtoni székhelyű, ötven éves múltra visszatekintő Center for Strategic & International Studies (CSIS) intézmény 2015-ben kiadott „North Korea’s Cyber Capabilities”, valamint a „North Korea’s Cyber Operations: Strategy and Responses” című kiadványaira, amelyek mértékadó dél-koreai és angol nyelvű tudósítások, valamint disszidensek beszámolóí alapján kerültek összeállításra.

A Koreai Népi Demokratikus Köztársaság politikai és katonai stratégiájának megértéséhez szükséges röviden áttekinteni, hogyan alakult a Koreai-félsziget történelme az elmúlt közel hatvan évben.

Japán 1910-ben hivatalosan annektálta Koreát. A II. világháború végén az Egyesült Államok és a Szovjetunió együtt harcolt a japán megszállók ellen, aminek következtében 1945-ben Korea felszabadult, és a Potsdami konferencián a szövetséges nagyhatalmak megállapodtak abban, hogy az országot a 38. szélességi fok mentén kettéosztják, és így kialakult a szovjet és az amerikai érdekszóna. Hasonlóan Európához, a megszállási zónáknak megfelelően kommunista és tőkés érdekszónák jöttek létre. Délen 1948. augusztus 15-én létrejött a Koreai Köztársaság, majd ezt követően szeptember 9-én kiáltották ki a Koreai Népi Demokratikus Köztársaságot. Északon szigorú kommunista diktatúra jött létre, míg délen egy antidemokratikus társadalmi berendezkedés alakult ki, amely csak az 1980-as évek második felében vált nyitottabbá. A két Korea között 1950 és 1953 között kínai, orosz és amerikai résztvevőkkel háború dúlt, amely azonban nem békekötéssel, hanem azóta is tartó tűzszünettel zárult. A két országot elválasztó demarkációs vonal is nagyjából az eredeti helyén lett kijelölve.

Az ezredfordulót követően Dél-Koreában óriási gazdasági fellendülés következett be, míg északon a diktatúra konzerválódott, a világtól elzárt katonai állam jött létre, ahol a kommunizmus még mindig teljhatalommal bír.³

¹ A szerző a Honvéd Vezérkar Tudományos Kutatóhely külsős kutatója.

² Rövidítve: KNDK, a tanulmányban a földrajzi elhelyezkedése kapcsán az Észak-Korea megjelölést is használom

³ HARMAT Árpád Péter. "Korea kettészakadásának története." *Történelemcikk.hu*. 2015.06.20. <http://tortenelemcikk.hu/node/372>. (Letöltés ideje: 2017.05.21.)

A tüzszünet megkötésétől a 80-as évek végéig az erőegyensúly a térségben az északi félnek kedvezett. Azonban az egyre mélyülő belső válság, a költségvetési nehézségek, és a hidegháború végeztével a Szovjetunió és Kína támogatását elveszítve az erőegyensúly a déli oldal felé billent, így Észak-Koreának az addigi katonai stratégiáját meg kellett változtatnia és a korábbi hagyományos hadviselés helyett a hangsúlyt az aszimmetrikus hadviselésre helyezte. Jelenleg Észak-Koreának van a világon az egyik legnagyobb létszámú különleges műveleti erőkből álló hadereje. Számos szabotázsakciót hajtottak már végre a déli szomszéd ellen, beleértve magas beosztású vezetők meggyilkolására irányuló akciókat is.⁴ A különleges műveleti erők háború esetén a hagyományos erőkkel együtt kerülnének alkalmazásra főleg az ellenség mélységében és a háterszágában vezetési pontok ellen, illetve a polgári lakosság körében szabotázsakciókat és merényleteket hajtanának végre.⁵ A stratégiájuk alapja a „gyors háború, gyors befejezés”. Számításaik szerint a háborút a céljaik elérésével még az előtt be kell fejezniük, hogy az amerikai fél segítsége megérkezne.

Észak-Korea békeidőben is folyamatosan provokálja a déli szomszédját olyan műveletekkel, amelyek nem érik el a háborús küszöböt, de folyamatosan nyomás alatt tartják az ellenséget, és igyekeznek a morálját megrendíteni. A relatíve kisebb befektetéssel fenntartható provokáció és fenyegetés eszközei az interkontinentális ballisztikus rakéták, az atomfegyver és az informatikai hadviselés.

Észak-Korea kiberstratégiája

Az ország politikai és katonai stratégiája ez idáig nem került nyilvánosságra. A kutatók mindössze a helyi hírekből és a Koreai Munkáspárt értekezleteiről készült beszámolókból valószínűsítik, hogy a szóban forgó doktrínák és stratégiák az egykori Szovjetunióban végzett politikusok, katonák és szakemberek hatására rokon vonásokat mutathat a korábbi szovjet doktrínákkal és stratégiákkal, amelyeket az egyedi igényeiknek megfelelően kissé módosíthattak. A részletek ismerete nélkül két fontos, jól elkülöníthető elvet azonosítottak, amelyek nagy valószínűséggel a katonai stratégia részei lehetnek. Az egyik az ellenség hagyományos műveleteinek akadályozása, a másik pedig a békeidőben folytatott folyamatos háború küszöb alatti provokáció, amellyel az ellenség morálját kívánják megtörni.

Az észak-koreai elemzők tanulmányozták a közelmúltban vívott háborúkat és megállapították, hogy az amerikai fél nagymértékben támaszkodik korszerű vezetési irányítási rendszereire (C4ISR), illetve a déli szomszédjuk is egyre szélesebb körben alkalmazza a számítógépes hálózatokat és az Internetet az élet minden területén, így sebezhetővé váltak. Ez a felismerés vezette a döntéshozókat arra a következtetésre, hogy viszonylag kis befektetéssel nagy eredményeket érhetnek el, amennyiben sikerül olyan potenciált kifejleszteniük, amellyel sikerrel béníthatják, illetve pusztíthatják a számítástechnikai rendszereket. Tisztában vannak azzal, hogy egy esetleges háborút nem lehet kibereszközökkel megnyerni, de nem is ez a céljuk.

⁴ Victor CHA – James Andrew LEWIS: "North Korea's Cyber Capabilities." North Korea's Cyber Capabilities Center for Strategic and International Studies. December 18, 2014. p. 26., <https://www.csis.org/programs/korea-chair/north-koreas-cyber-capabilities> (Letöltés ideje: 2017. 05.20.)

⁵ CHA – LEWIS i.m. p. 12.

Mindezek szellemében az aszimmetrikus stratégiájuk szerves részeként kidolgozták kiberstratégiájukat.

Az ország kibertevékenységét a Koreai Népi Hadsereg Vezérkara⁶ és az Általános Felderítő Iroda, valamint a Koreai Munkáspárt koordinálja. Tekintettel arra, hogy hivatalos iratok nyíltan nem hozzáférhetők, a kiszivárgott értesülések szerint a három szervezet valamilyen szempontrendszer szerint a felelősségi területeket felosztva szervezi és irányítja az ország kibertevékenységét. Úgy tűnik, hogy a Koreai Népi Hadsereg kiberegységei az elektronikai harcegységek állományából kerültek kialakításra, míg a Felderítő Iroda kiberegységeit a korábban felderítő, provokációs és különböző köztörvényes bűnügyek elkövetésére szakosodott állomány bázisán hozták létre. Az Egyesült Államok és a Dél-Koreai Köztársaság elleni kibertámadásokért a Felderítő Irodát teszik felelőssé. A sajtóban megjelent hírek szerint az észak-koreai vezetők a kiberképesség fejlesztésére hívták fel a vezérkar figyelmét, ebből elemzők arra következtetnek, hogy a Felderítő Iroda fejlettebb kiberképességekkel rendelkezik, mint a vezérkar.⁷

Dél-koreai források szerint a békeidőben végrehajtott provokációkért az Általános Felderítő Iroda a felelős.⁸

Észak-Korea kiberszervezetei

A következőkben egy nagybani képet mutatok be a kibertevékenységben érintett szervezetekről, az alá-fölérendeltségi viszonyokról. Az információs hadviselés jellegéből adódóan nem lehet megbecsülni, hogy mennyi és mennyire fejlett eszközzel rendelkeznek, hiszen ezek az eszközök nem vethetők össze ilyen értelemben a hagyományos fegyverzettel. Mindazonáltal az országnak tulajdonított műveletek egyfajta képet adhatnak a képességeikről, illetve felkészültségükről.

Általános Felderítő Iroda

A Koreai Népi Demokratikus Köztársaság hírszerző szerve, amelyet a szakértők a kibertevékenység központjának tartanak és a hagyományos hírszerzési feladatokon túl terrorakciókkal, valamint békeidőben elkövetett fegyveres provokációkkal, emberrablásokkal és más illegális műveletekkel hoznak kapcsolatba. A Felderítő Iroda irányítása alá rendelt kibertevékenység azt jelenti, hogy a politikai vezetés ezt a hadviselési módot a nemzeti célok megvalósítása egyik fő eszközének tekinti.

A Munkáspárthoz, illetve a Honvédelmi Minisztériumhoz tartozó hírszerző és kibertevékenységet folytató szervek egy részét 2009 és 2010 között átszervezték és többek között ezekből hozták létre az Általános Felderítő Irodát.

Az Iroda közvetlenül a Nemzeti Védelmi Tanácsnak számol be tevékenységéről, de nem tudni, hogy a Védelmi Tanács milyen mértékben felügyeli. Nem ellenőrzött értesülések szerint a felső vezetők, beleértve Kim Dzsong-Un-t⁹ és

⁶ Korean People Army General Staff Department (KPA GSD)

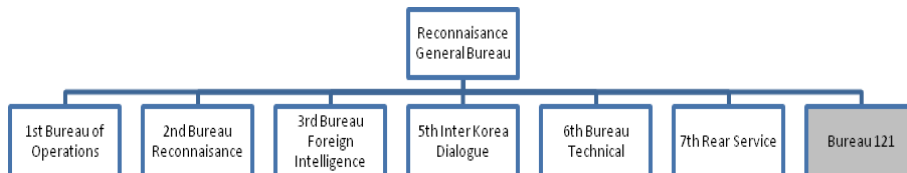
⁷ CHA – LEWIS i.m. p. 26.

⁸ CHA – LEWIS i.m. p. 34.

⁹ A Koreai Népi Demokratikus Köztársaság legfőbb vezetője, neve magyarul „Igaz Kegyelem”-et jelent

O Kuk-Ryol¹⁰-t személyesen irányítják a 121-es Igazgatóságot, amely a Felderítő Iroda kibertevékenységgel foglalkozó igazgatósága.

Mint az alábbi ábrán is látható, a Felderítő Iroda hét igazgatóságból áll: Műveletek, Felderítő, Külföldi hírszerző, Koreák közötti párbeszéd, Műszaki, Támogató, valamint a már említett 121-es Igazgatóság. Az igazgatóságok neve nem feltétlenül utalhat a tevékenységükre, mivel ezek az átszervezésnél egybeolvasztott elődök nevei. Elképzelhető, hogy a nevek megmaradtak, de a tevékenységi profil már megváltozott.



1. ábra Az Általános Felderítő Iroda szervezeti felépítése¹¹

Az Általános Felderítő Iroda számos fedőcéget is működtet, amelyek fegyverkereskedelemmel, kereskedelemmel, technikai beszerzésekkel foglalkoznak.

Az Általános Felderítő Iroda kiberrészlegei

Az ország részéről tapasztalható titkolózás és félrevezető szándékok miatt lehetséges, hogy egyes szervezetek neve, esetleg tevékenysége időről-időre megváltozik, de mindezen korlátok mellett is egyfajta általános képet kaphatunk a belső felépítésről és működésről.

1. 121-es Igazgatóság (Elektronikus Felderítő és Kiberhadviselési Igazgatóság)

A 121-es Igazgatóság a KNDK legfontosabb kiberszervezete. A tevékenysége magába foglalja a hírszerzési, elhárítási, valamint a védelmi és támadó jellegű kiberműveletek, hálózati hadviselési és kiberbűnözési tevékenységét. Különböző források különböző neven hivatkoznak rá, mivel az eltérő hivatalos koreai megnevezések is az állami megtévesztés részét képezik. Észak-koreai disszidensek beszámolóí szerint Észak-Phenjanban 2013 májusában egy új, modern főhadiszállást építettek az Igazgatóságnak néhány luxuslakással, amelyekben az alkalmazottak kerültek elhelyezésre. A műholdképek elemzése nem erősíti meg ezt az információt, azonban nem lehetetlen, hogy a létesítmény jelentős részét a föld alatt helyezték el, mivel ez bevett gyakorlat a számukra különösen fontos létesítmények esetében.¹²

¹⁰ A Nemzeti Védelmi Tanács alelnöke

¹¹ CHA – LEWIS i.m. p. 41.

¹² CHA – LEWIS i.m. p. 41.

2. Számítástechnikai Kutató Laboratórium

A laboratórium neve először 2013. május 20-án hangzott el nyilvánosan, amikor Nam Jae-Joon, a dél-koreai hírszerző szolgálat vezetője kongresszusi meghallgatásán kijelentette, hogy a Számítástechnikai Kutató Laboratórium és a 110-es Igazgatóság olyan hacker-képességgel rendelkezik, hogy károkozó támadásokat indíthatnak dél-koreai pénzügyi intézmények ellen. A szervezetek sorsa azóta ismeretlen, átszervezhetők, vagy átnevezhetők őket, azonban mindenképpen érdemes megemlíteni őket, mivel egy dél-koreai internetes számítástechnikai magazin egy disszidens beszámolója alapján megírta, hogy a Számítástechnikai Kutató Laboratórium Észak-Phenjaban került elhelyezésre a Koreai Központi Hírügynökség épületében és Jo Myung-Lae ezredes vezeti, akinek a nevéhez fűződik a 2000-es évek elején a JML vírus (továbbiakban: JML) kifejlesztése. Jo Myung-lae ezredes a Mirim Katonai Főiskolán végzett 1997-ben, ahol a számítógépes vírusok katonai alkalmazása nevű szakon szerzett diplomát.

3. Első Műveleti Igazgatóság, 414-es Összekötő Hivatal, 128-as Összekötő Hivatal

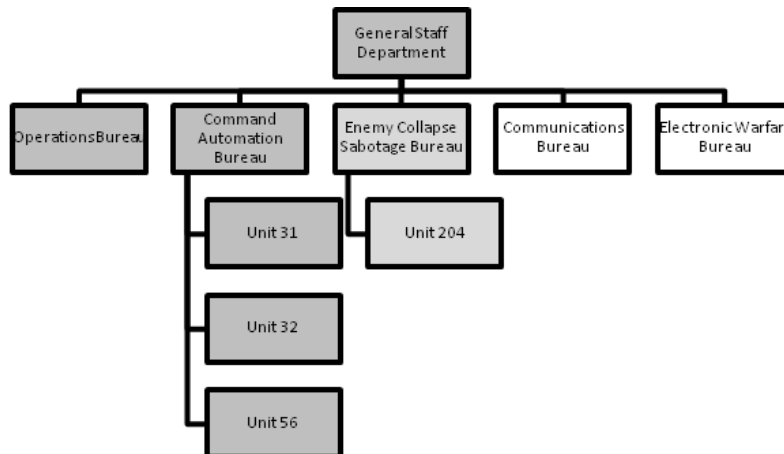
A koreai terminológiában az „összekötő” szó a hivatalok nevében a Dél-Koreába indított kommandóakciók idején a különleges egységekkel történő kapcsolattartásra, és a külföldi hírszerzőkkel, valamint ügynökökkel fenntartott összeköttetésre utal. A 414-es egység ma már nem csak a kapcsolattartásért felelős, hanem a kiberhírszerzésért is, ezen belül pedig a déli szomszéd katonai és rendfenntartó egységei irányába folytatott technikai, és ezen belül kiemelten a kibertérben történő információgyűjtésért is.

A Koreai Népi Hadsereg Vezérkara

A vezérkar feladata és rendeltetése megegyezik általában más vezérkaroknál megszokottakkal. A Vezérkar felett névleges hatalmat gyakorol a Honvédelmi Minisztérium, azonban a vezérkar igazi parancsnoka a Koreai Népi Hadsereg főparancsnoka Kim Dzsong-Un, a legfőbb pártvezér.

A vezérkar kibertevékenységgel kapcsolatban rendkívül kevés információ kerül nyilvánosságra, köszönhetően annak, hogy a vezérkari szervek nem érintettek a polgári lakossággal szembeni nagyszabású kibertámadásokban.

A kibertevékenységben érintett szervezeti egységei a következők: Műveleti Igazgatóság, Kommunikációs Igazgatóság, Elektronikai Hadviselési Igazgatóság, Parancsautomatizálási Igazgatóság, Ellenség Bomlasztó és Szabotázs Igazgatóság.



2. ábra A vezérkar kibertevékenységben érintett igazgatóságai¹³

Műveleti Igazgatóság

A Műveleti Igazgatóság nem hajt végre önállóan műveleteket, de meghatározó szerepe van a kibererők stratégiai célú alkalmazásának és egyes feladatokba történő bevonásának kidolgozásában. A vezérkar egyik legfontosabb szerve; egyes források tudni vélik, hogy a vezetője megkerülve a szolgálati utat, kihagyva a vezérkari főnököt, közvetlenül a haderő főparancsnokával van összeköttetésben.¹⁴

Parancsautomatizálási Igazgatóság

Az igazgatóság valószínűsíthetőleg számítógépes hálózati műveleteket hajt végre és kártevő-fejlesztéssel, valamint biztonsági rések felkutatásával foglalkozik. Az egységet a korai 1990-es években hozták létre, miután tanulmányozva az Öböl-háború amerikai vonatkozásait rájöttek, hogy a mindenkori pontos és precíz információk beszerzéséhez és azok továbbításához szükséges informatikai eszközök és hálózatok sebezhetővé teszik az ellenséget. Az igazgatóság állománya mintegy 60 fő tisztből áll. Az igazgatóság 31-es egysége a kártevő fejlesztéssel, az 56-os egysége a katonai célú szoftverek fejlesztésével foglalkozik.

A már említett észak-koreai disszidensek szervezete szerint ezeket az egységeket bevonták az Általános Felderítő Iroda által irányított akcióba, melynek feladata a robbanófejek miniaturizálása és a ballisztikus rakéták fejlesztéséhez szükséges technológia ellopása volt.

¹³ CHA – LEWIS i.m. p. 41.

¹⁴ Uo. p. 46.

Az Ellenséget Bomlasztó és Szabotázs Igazgatóság¹⁵

A szervezetet főleg propagandacélokból hozták létre, és amennyiben végrehajt valamilyen számítógépes hálózati műveletet, azt csak és kizárólag propaganda célokból teszi.

Az Igazgatóság három dandárból áll, dandáronként mintegy 600-700 fővel. A vezetője hadosztályparancsnok, altábornagyi rendfokozattal. Az igazgatóságot 563. Katonai Egységnek is hívják. A feladata békeidőben a dél-koreai árulók toborzása, az északi propaganda terjesztése és harmadik országból történő behatolás előkészítése Dél-Koreába. Háborús feladata dél-koreai katonának öltözve bejutni az ellenség soraiba, és onnan akadályozni a déliek műveleteit, valamint szabotázs tevékenységek elkövetésével demoralizálni az ellenség sorait.

Kommunikációs Igazgatóság

Az Igazgatóság szervezeti felépítése és létszámviszonyai nem ismertek. A rendelkezésre álló adatok szerint ez a szervezet felügyeli a hadsereg teljes belföldi és külföldi kommunikációját. Az igazgatóság együttműködik a Biztonsági Minisztériummal, rádió-felderítő feladatok ellátása során együttműködik az Általános Felderítő Irodával, valamint a Minősített Információk Igazgatóságával, felelős a titkosított kommunikációért. Az állomány képzését a Kommunikációs Tiszti Akadémia végzi.

Elektronikai Hadviselési Igazgatóság

Az igazgatóság felügyeli a hadsereg elektronikai harci tevékenységét. A szervezetet jelentések szerint a hadsereg modernizálásának keretében az 1980-as évek közepén hozták létre. A dél-koreai Honvédelmi Minisztérium 2005-ös jelentése szerint az Igazgatóság alá tartozik egy négy zászlóaljából álló elektronikai harc ezred.

A szervezet rendeltetése az elektromágneses spektrumban az ellenség vezetési és irányítási rendszerének zavarása és pusztítása. A közelmúlt eseményei azt mutatják, hogy az észak-koreai hadsereg igyekszik folyamatosan tesztelni és fejleszteni az elektronikai harc eszközeit.

Jó példa erre, hogy 2010-ben a zavarvédelemmel nem biztosított dél-koreai radarokat zavarással bénították meg, miközben tüzérségi tűz alá vették a Yeonpyeong-szigetet. A déli fél nem tudta bemérni az északi tüzérségi eszközeit, így a régi koordináták alapján leadott válaszlövésekben kilőtt gránátok 80%-a tengerbe csapódott be. Két évvel később a Koreai Köztársaság sajtójában több tudósítás is megjelent arról, hogy az északi fél az ország nyugati felében megpróbálta megzavarni a GPS eszközöket. Ilyen kísérletet egyébként több alkalommal is jeleztek. Déliek tájékoztatása szerint a precíziós fegyverek nem kerültek veszélybe, mivel azok védve vannak az ilyen jellegű zavarás ellen. A déli szakértők szerint kétféle berendezést alkalmaztak, az egyik orosz gyártmányú, a

¹⁵ A dél-koreai sajtó kiberszervezetnek nevezi, de valójában ez egy információs és lélektani hadviselési egység.

másik pedig egy Észak-Koreaiak által módosított, szintén orosz gyártmányú eszköz volt. Ez utóbbit eladásra kínálták több Közel-Keleti országnak.

A vezérkarnak más országoktól eltérően nincs a kiberhadviselésért felelős központi egysége, ha létezik is ilyen, az nem került nyilvánosságra. Úgy tűnik, hogy az ilyen feladatokat az Általános Felderítő Iroda látja el, amely viszont nincs függőségi viszonyban a vezérkarral.

A vezérkart sem az Egyesült Államok, sem pedig a Koreai Köztársaság részéről nem hozták ez idáig összefüggésbe semmilyen kibertámadással.

Az ipari és technológiai alapok

Első pillantásra Észak-Korea informatikai fejlettsége sokakat megmosolyogtat, hiszen a háztartásokban kevés személyi számítógép van, és még kevesebb az Internet-hozzáféréssel rendelkezők száma. A technikai és technológiai fejlettségét vizsgálva már gyökeresen más képet kapunk. Ez az ország az elmúlt húsz évben gondos és tervszerű fejlesztő munkával olyan képességeket szerzett, amelyekkel sikeresen támadhat a világban bárhol polgári és katonai informatikai rendszereket.

Észak-Korea az 1980-as évek második felében kezdte el informatikai képességeit fejleszteni, de az igazi áttörés az 1990-es évek végén következett be. Ekkor jelölték ki az 1999-es évet a tudomány évének és ennek keretében létrehozták a Kim Il-sung Egyetem Számítástechnikai Főiskolai karát és a Villamos és Energiaügyi Minisztériumot. Azóta négy ötéves tervet indítottak, amelyeknek fő céljaként a tudomány fejlesztését határozták meg, azon belül is számítástechnikai haladásra helyezték a hangsúlyt. A különböző kormányzati szervek mellett a Posta és Kommunikációs Minisztérium, és a Villamos és Energiaügyi Minisztérium felügyeli az informatikai fejlesztéseket. Ez utóbbi felügyeli az informatikai területhez tartozó félvezetőgyártást és hardverfejlesztést, valamint a számítástechnikai kutató intézeteket.

Észak-Korea a szoftverfejlesztésre helyezi a hangsúlyt. A képzésük olyan szintet ért el, hogy vendégmunkásként mérnökcsoportokat küldenek a kínai Shenyang-ba az informatikai fejlesztés egyik fellegvárába, ahol a Koreai Köztársaság¹⁶ részére fejlesztenek szoftvereket. Az állam a mérnökök fizetéséből egy részt elvesz, de az ide vezényelt dolgozók cserébe hozzáférnek a legkorszerűbb technológiákhoz, amelyek birtokában hazatérve jobb állásokra számíthatnak.

Észak-Korea a hardverfejlesztést sem hanyagolja el. A Phenjan-i Nyomatott Áramköri Lapok gyára és a Tanchon Katonai Félvezető gyár állítja elő az elektrotechnikai alkatrészeket és félvezetőket, valamint a belső piacra szánt mobiltelefonokat és tableteket.

A Koreai Népi Demokratikus Köztársaság két különálló blokkban összesen 1280 db IP-címet használ. Az egyik blokkot egy taiwani telekommunikációs cégtől,

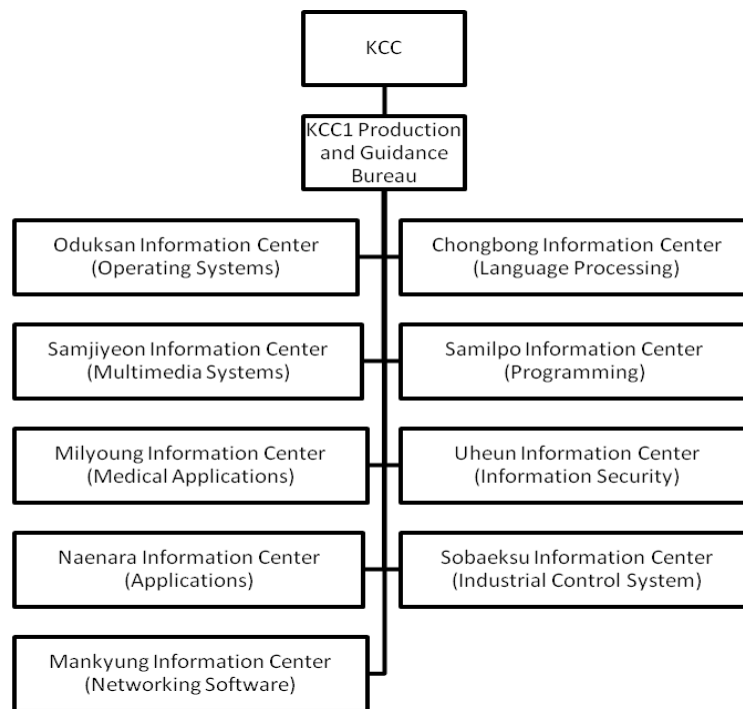
¹⁶ Felhívom a figyelmet arra a körülményre, hogy az ellenséges déli szomszéd részére fejlesztenek szoftvereket, ezáltal tisztában vannak annak minden gyengeségével, hátrányával, nem beszélve arról a lehetőségről, hogy hátsó kapukat, kártevőket építhetnek az általuk fejlesztett szoftverekbe.

a másikat pedig egy kínai vállalatától bérlik. Az állami honlapok ezeken az IP-tartományokon kerültek elhelyezésre.

Az országban négy különálló intranet hálózat működik. Az egyik katonai, a másik három pedig kormányzati célú hálózat. Természetesen a hálózatok szigorú ellenőzés alatt állnak. A hardver és szoftverfejlesztés magját két informatikai központ képezi, az egyik a Koreai Számítástechnikai Központ, a másik pedig a Phenjani Számítástechnikai Központ.

Koreai Számítástechnikai Központ

A Központot 1990. október 24-én hozták létre. Feladatául a kutatás-fejlesztés mellett a hardver- és szoftvergyártást, valamint az egyetemi szintű informatikaoktatás felügyeletét határozták meg. A központ külkereskedelmi joggal rendelkezik, a saját termékeit értékesítheti a nemzetközi piacokon. A létszáma hozzávetőleg mintegy 1200 fő, amelyből körülbelül 100 személy rendelkezik doktori fokozattal. Egyes tájékoztatások szerint vannak képviselői és közös vállalatai Németországban, Kínában és Szíriában. Legismertebb termékük a „Vörös Csillag” néven forgalmazott Linux disztribúció.



3. ábra A Koreai Számítástechnikai Központ szervezeti felépítése¹⁷

¹⁷ CHA – LEWIS i.m. p. 46.

A központ Kínában dolgozó munkatársai 2011-ben bűncselekmény gyanújába keveredtek, mivel a dél-koreai ügyészség vádat emelt öt dél-koreai állampolgár ellen, akik az országban népszerű számítógépes játékokhoz olyan szoftvereket vásároltak tőlük, amelyekkel manipulálni lehetett a játékok menetét. Ezeket a programokat később pénzért árulták Dél-Koreában. Önmagában nem ez képezte a bűncselekmény alapját, hanem az a tény, hogy a szoftverek az eredeti funkciójukon kívül alkalmasak voltak a telepítésüket követően az adott számítógép távolról történő vezérlésére, ezáltal úgynevezett botnet hálózatok létrehozására, illetve a számítógépen tárolt adatok megszerzésére, továbbá az eszközön végzett tevékenység megfigyelésére is. A tárgyaláson elhangzott, hogy a szoftvereket az észak-koreai Számítástechnikai Központ Kínában működő fedőcégeinek munkatársai fejlesztették. Megemlítték azt is, hogy Kínában mintegy tízezer észak-koreai informatikus szakember dolgozott abban az időben.

Ez az információ a bűnügyi vonatkozásokon túl azért érdemel figyelmet, mert bepillantást enged a Központ tevékenységébe. A történetek alapján megállapítható, hogy a Központ a már említett feladatain túl részt vesz a kibertámadások végrehajtásában, illetve nyilvánvalóvá vált, hogy a központ által üzemeltetett fedőcégeket felhasználják a kibertámadásokat végrehajtó állomány törvényes hátterének biztosítására.¹⁸

Phenjani Számítástechnikai Központ

A központot 1986 júliusában hozták létre Phenjanban az Oszakai Közgazdaságtani és Jogi Egyetem Informatikai Központjának mintájára. A Központ legfőbb feladata a szoftverfejlesztés. Hozzávetőleg 520 fős az állománya, ebből mintegy 30 fő rendelkezik tudományos fokozattal. Az átlagos életkor 20 és 30 év közötti. A szervezet nevéhez fűződik többek között az országban elterjedt Changduk nevű szövegszerkesztő program, valamint egy koreai nyelvet értelmező és feldolgozó program fejlesztése. A Központ irodákat működtet Szingapúrban és Japánban, azonban ellenséges kibertevékenységre utaló információ ezidáig nem keletkezett vele kapcsolatban.

A Phenjani Informatikai Központ a 2000-es évek elején részt vett a dél-koreai „Napsugár politika” elnevezésű politikai kezdeményezés keretében létrehozott „Koreák közötti informatikai együttműködés” néven indított programban. A kezdeményezés célja a közös alapokon nyugvó kutatás-fejlesztés, illetve a közös szoftverfejlesztés kialakítása volt. Az együttműködés azonban fokozatosan gyengült, miután Észak-Korea 2006-ban sikeres kísérleti atomrobbantást hajtott végre, majd miután 2010. március 26-án feltételezhetően az északiak megtorpedóztak egy déli hadihajót, a program be is fejeződött. Az incidenst követően a Koreai Köztársaság megtiltott minden kereskedelmi, gazdasági, valamint humanitárius együttműködést az északi féllel.

Az észak és dél együttműködésének szemléletes példája volt a 2001-ben a kínai Dandongban létrehozott „Hana Program Központ” elnevezésű vegyesvállalat,

¹⁸ Jenny JUN – Victor D. CHA – James A. LEWIS – Scott LAFOY – Ethan SOHN: North Korea's cyber operations: strategy and responses. Washington DC: Center for Strategic & International Studies, 2015. p. 54.

amelyet Kínában hozott létre a Phenjani Informatikai Központ és a dél-koreai Hanabiz konzorcium. A vállalkozás fő profilja a szoftverfejlesztés volt, elsősorban a dél-koreai megrendelők részére. Az elképzelések szerint a déli partner biztosította a tőkét, az északi fél pedig a szakembergárdát. A távlati céljaik között szerepelt, hogy Dandongban egyfajta Szilikon-völgyet hoznak létre. A vállalkozás a megrendelések hiányában és a politikai helyzet alakulása miatt 2011-ben csődbe ment, azonban ez az együttműködés lehetőséget teremtett arra, hogy az északi szakemberek felkészültségéről és tudásszintjéről ismereteket szerezhessünk, ugyanis a déli fél az állami támogatás felhasználásának ellenőrzése céljából többször is ellenőrizte a központ működését és ezekről jelentéseket is készítettek. A több, egymástól független jelentés az északi szakemberek felkészültségét nagyon jónak értékeli, és kiemelik, hogy a déli munkatársakhoz képest sokkal elhivatottabbnak és kitartóbbnak bizonyultak. Az egyetlen hiányosságuknak a felhasználói felület fejlesztését tartották, de ezt azzal magyarázták, hogy ezek a szakemberek nem szoktak hozzá a piaci célú szoftverfejlesztéshez, amelynek értelemszerűen fontos eleme a felhasználóbarát kezelőfelület készítése. Fontosnak tartották megjegyezni, hogy az északiak sokkal képzetebbek az információvédelmi technológiák területén.

Záró gondolatok

Észak-Korea kiberszervezeteinek bemutatásával a tanulmány első részének a végéhez érkeztünk.

Az eddig bemutatottak alapján látható, hogy a politikai vezetés számos más országot megelőzve megérezte az „idők szavát” és a rendelkezésre álló szűkös erőforrások átcsoportosításával, valamint nagyfokú előrelátással magasan képzett polgári és katonai informatikus szakembergárdát hozott létre. Ennek az állománynak a bázisán a stratégiai céljaik elérése érdekében megszervezték a polgári és katonai titkosszolgálatok kiberhadviselő szervezeteit, amelyek egymással szoros együttműködésben végzik feladatukat és vezetésük egységes elgondolás alapján, központi akarattal történik. A szervezetek felkészültségét és hatékonyságát kellően illusztrálja majd a tanulmány második részében bemutatásra kerülő híres-hírhedt Lazarus csoport és annak tevékenysége, illetve néhány olyan nemzetközi visszhangot kiváltó kiberművelet, amely ennek a csoportnak a számlájára írható. Mint az majd kiténik, ezek a műveletek megalapozzák értékelésünket, miszerint az ország helyet követelhet a fejlett kiberhadviselő országok élmezőnyében.

Felhasznált irodalom:

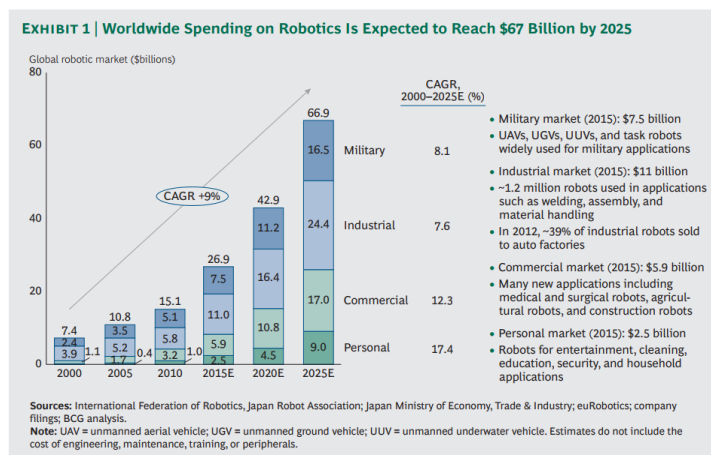
- HARMAT Árpád Péter: Korea kettészakadásának története Tortenelemcikk.hu. 2015. 06. 20., <http://tortenelemcikk.hu/node/372>. (Letöltés ideje: 2017. 05. 21.)
- CHA, Victor– James Andrew LEWIS: North Korea's Cyber Capabilities. North Korea's Cyber Capabilities Center for Strategic and International Studies. 2014. 12. 18, <https://www.csis.org/programs/korea-chair/north-koreas-cyber-capabilities>. (Letöltés ideje: 2017. 05. 20.)

- Kaspersky Lab's Global Research & Analysis Team. "LAZARUS UNDER THE HOOD." Securelist. 2017.04.03. <https://kas.pr/ix6C> (Letöltés ideje: 2017. 05. 20.)
- KEANE, Justin C. Klein: PHP Malware C99 Shell. "Mad Irish . net." Mad Irish, <http://www.madirish.net/241>. (Letöltés ideje: 2017. 05. 20.)
- KNF – Komisja Nadzoru Finansowego [,https://www.knf.gov.pl/opracowania/sektor_bankowy/index.html](https://www.knf.gov.pl/opracowania/sektor_bankowy/index.html) (Letöltés ideje: 2017. 05. 20.)
- Novetta: Operation „Blockbuster”, <https://www.operation„Blockbuster”.com/wp-content/uploads/2016/02/Operation-„Blockbuster”-Report.pdf>, (Letöltés ideje: 2017. 05. 20.)
- Ryan SHERSTOBITOFF and ITAI Liba, McAfee® Labs and James WALTER, Offie of the CTO: Dissecting Operation Troy: Cyberespionage in South Korea, McAfee Labs, 2013. <https://www.mcafee.com/error-pages/404.aspx?url=https://www.mcafee.com/kr/resources/white-papers/wp-dissecting-operation-troy.pdf> (Letöltés ideje: 2017. 05. 21.)
- SHEVCHENKO, Sergei: BAE Systems Threat Research Blog. Cyber Heist Attribution. 2016.01.13. <http://baesystemsai.blogspot.hu/2016/05/cyber-heist-attribution.html> (Letöltés ideje: 2017. 05. 20.)
- "Indiana University Indiana University Indiana University." What is a Master Boot Record (MBR)? Accessed June 09, 2017. <https://kb.iu.edu/d/aijw>. (Letöltés ideje: 2017. 05. 20.)
- North Korea's Cyber Operations: Strategy and Responses. North Korea's Cyber Operations: Strategy and Responses | Center for Strategic and International Studies. November 23, 2015. <https://www.csis.org/events/north-korea%E2%80%99s-cyber-operations-strategy-and-responses> (Letöltés ideje: 2017. 05. 20.)
- The global provider of secure financial messaging services, <https://www.swift.com/about-us/discover-swift> (Letöltés ideje: 2017. 05. 20.)
- "What Do We Know About Past North Korean Cyber Attacks and their Capabilities?", Center for Strategic and International Studies, <https://www.csis.org/analysis/what-do-we-know-about-past-north-korean-cyber-attacks-and-their-capabilities>. (Letöltés ideje: 2017. május 20.)
- Windows Sysinternals System Monitor (Sysmon), Technet Microsoft, <https://technet.microsoft.com/en-us/sysinternals/bb545027.aspx> (Letöltés ideje: 2017. 05.31.)

A SZOLGÁLTATÓ ROBOTIKA HELYZETE ÉS KUTATÁSI IRÁNYAI

Robotpiaci előrejelzések

A termelői ipar után a hadiparban a legnagyobb mértékű a robotokkal kapcsolatos fejlesztésekre fordított források mértéke. Az International Federation of Robotics¹ előrejelzésében látható, hogy míg a személyes használatú robotok ugrásszerűen törnek be a piacra, addig a hadiparban egy régóta tartó erőteljes növekedés figyelhető meg. 2025-re az előrejelzés szerint a szolgáltató robotokra 9 milliárd, míg a hadiparban használatos robotokra 16,5 milliárd dollárt fognak költeni világszerte. Már 2015-ben is, amikor a legutóbbi előrejelzés készült² a hadiparban már széles körben használtak célfeladatokra tervezett robotokat, valamint külön megnevezés nélküli légi (UAV)-, szárazföldi (UGV)-, valamint víz alatti (UUV) robotizált járműveket, melyek alkalmazási területe és mértéke napjainkban még jelentősebb lett (1. ábra).



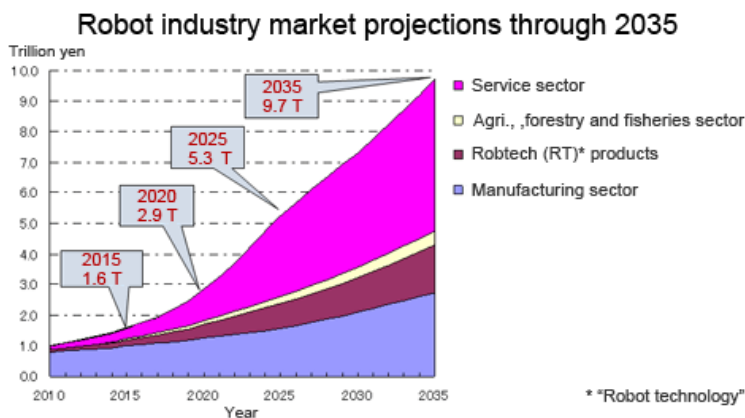
1. ábra: Robotikai fejlesztésekre fordított források alakulása 2000 és 2015 között³

¹ IFR: World Robotics Survey, IFR International Federation of Robotics, <https://ifr.org/ifr-press-releases/news/world-robotics-survey-service-robots-are-conquering-the-world-> (Letöltés ideje: 2017. 09. 07.)

² BÉKÉSI, Bertold– Péter SZEGEDI: Napjaink fegyverrendszer fejlesztési trendjei. *Economica* (1585-6216) 2015/8. pp. 158-168., <http://eds.b.ebscohost.com/abstract?site=eds&scope=site&jrnl=15856216&AN=113875035&h=3B8JwiRgkvTYGCoSfNF42C%2fjeNzWyqGaPty1nu4z5fe9EIdVOsIKwrnfEoW1qja1oLcRoHYWD1ZQIM7nV1HBCQ%3d%3d&crl=c&resultLocal=ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d15856216%26AN%3d113875035>. (Letöltés ideje: 2017. 09. 27.)

³ SANDER, Alison – Meldon Wolfgang: The rise of robotics, The Boston Consulting Group, 2014/27. http://img-stg.bcg.com/The_Rise_of_Robotics_Aug_2014_tcm9-82495.pdf. (Letöltés ideje: 2017. 10. 27.)

A Japán gazdasági hivatal, a METI jelentése szerint^{4,5} a robotpiacon a következő évtizedekben jelentős bővülés, valamint átrendeződés lesz megfigyelhető (2. ábra). Az alacsony születési szám és az öregedő népesség Japánban fejt ki legerősebben hatását, de a fejlett Európai és Amerikai országokban is számottevő az ebből következő munkaképes népesség csökkenése és a hosszú élettartamból adódó szociális ellátás növekedése. Ezen hatások együttes kezelésére a robotok alkalmazása jelentős potenciált rejt. A robotika területén megfigyelhető verseny háttérében az IoT (Internet of Things – Dolgok Internete) játszik meghatározó szerepet a digitális információ és virtuális hálózatok által. A robotok gyakorlati és specializált alkalmazásain keresztül rendelkezésre álló hatalmas mennyiségű információ elősegíti a robotok térnyerését az adat alapú innovációs korszakban. Katonai összefüggés lehet az előerő védelme, az alacsonyabb létszámú haderő szükségessége, valamint speciális műveleti képességek kialakítása.



2. ábra: Robotpiaci trendek alakulása

A Nemzetközi Robotikai Szövetség (IFR) 2016-os jelentése⁶ szerint 2015-ben 253.748 ipari robotot adtak el világszinten, ami a 2010 óta átlagos 16%-os növekedés eredménye. A 2019-es időszakban az előrejelzés szerint további átlagos 12% növekedés várható, ami az üzemben lévő robotok számát közel 2,6 millióra növeli (3. ábra). A hadiparban a Technavio előrejelzése szerint 11,75%-os

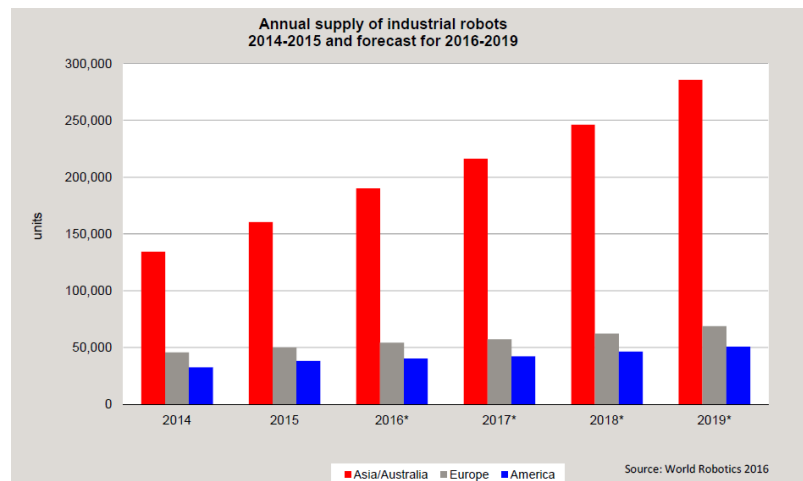
⁴ Ministry of Economics and Trade (METI): 2035nen ni muketa robotto sangyou no shourai shijou yosoku (Market forecast of robot industry in 2035). Ministry of Economics and Trade (METI), 2010. <http://www.meti.go.jp/press/20100423003/20100423003-2.pdf>. (Letöltés ideje: 2017. 10. 17.)

⁵ Ministry of Economy, Trade and Industry (METI): Announcement of the Results of a Trend Survey on the Robot Industry Market Japan Maintains the World's Top Market Share and the Chinese Market is Rapidly Growing, 2013. http://www.meti.go.jp/english/press/2013/0718_02.html. (Letöltés ideje: 2017. 09. 17.)

⁶ International Federation of Robotics: Executive Summary World Robotics 2016 Industrial Robots, World Robotics 2016. https://ifr.org/img/uploads/Executive_Summary_WR_Industrial_Robots_20161.pdf. (Letöltés ideje: 2017. 09. 07.)

növekedés várható a robotpiacon a 2017-2021-es időszakban⁷. Továbbá ebben az időszakban várható:

- az ipar 4.0 összeköti a virtuális valóságot a valódi termeléssel;
- áttörés az Ember-robot együttműködésben;
- kompakt és egyszerűen használható együttműködő robotok piaci térnyerése;
- a robotok javítják a munkakörülményeket, átvéve a veszélyes feladatokat az embertől;
- a katonai feladatok segítésében is fejlődés várható⁸
 - Jelenleg is alkalmaznak különféle UAV-okat felderítési céllal (pl. a magyar fejlesztésű BORA), melyek közül a várhatóan a kvadrokopterek szerepe fog nagyobb hangsúlyt kapni kiemelkedő tulajdonságai miatt
 - Szintén alkalmaznak tűzserész robotokat is, melyek emberélet veszélyeztetése nélkül képesek a bomba hatástalanítására;
 - Fontos még megemlíteni, hogy a különféle robotok az aktuális feladatok megfelelően felszerelhetők speciális eszközökkel, amelyek még alkalmasabbá teszik a feladat ellátására. Ilyen eszköz lehet például egy röntgenkeret, vegyi detektor, vagy rádióhullámokat zavaró egység;
- kis és Közép vállalatok egyre nagyobb mértékben használnak ipari robotokat;
- Közép-Európában nagymértékű, Nyugat-Európában pedig mérsékelt növekedés a robotok eladásában.



3. ábra: Robot eladások alakulása a 2014-2019 időszakban - IFR⁹

⁷ Technavio Co: Global Military Robots Market 2017-2021, Market Research. Infiniti Research Limited, 2017. <https://www.researchmoz.us/global-military-robots-market-2017-2021-report.html>. (Letöltés ideje: 2017. 10. 20.)

⁸ KOVÁCS Zoltán Tibor: Az improvizált robbanóeszközök elleni védelem elvei, módszerei és eljárásai, 2014. <http://real.mtak.hu/16086/1/Improviz%C3%A1lt%20robban%C3%B3eszk%C3%B6z%C3%B6k%20elleni%20v%C3%A9delem%20elvei%20m%C3%B3dszerei%20%C3%A9s%20elj%C3%A1r%C3%A1sai.pdf> (Letöltés ideje: 2017. 09. 27.)

A későbbiekben a jelenleg meghatározó klasszikus ipari robotok vezető szerepét átveszik a szolgáltató robotok, melyek 2035-re a teljes robotikai piac felét is kitehetik. Ez részben annak is köszönhető, hogy a korábbi, konvencionálisan nem robotnak nevezett eszközök egy része a szenzorok és a mesterséges intelligencia használatával újfajta robotokká alakulnak. Ilyen eszközök például a járművek (önvezető autók és pilóta nélküli repülőgépek) háztartási eszközök (otthon automatizálás) vagy éppen a mobiltelefonok (személyi asszisztens) is. A szakmai folyóiratokban és a konferenciákon már most is a legtöbb publikáció e területtel foglalkozik, elhanyagolható piaci szerepük ellenére, a bennük rejlő potenciál miatt. Az előrejelzés az irodai, egészségügyi, otthoni és hasonló területeken alkalmazott mobilrobotokkal kapcsolatban mutatja a legnagyobb fejlődést. Ebben Japán vezető szerepet tölt be azért, hogy nemzeti szinten határoz meg robotizálási stratégiát és tesz lépéseket annak 2020-ig történő megvalósítására⁹.

Katonai területen is hatalmas jelentősége van a robotok alkalmazásának. Egyfelől tökéletes parancs-végrehajtók, másfelől mindenféle morális kérdések felmerülése nélkül utasíthatóak életveszélyes feladatok végrehajtására. Egy, a körülményekhez optimalizált robot számára nincsenek nehezen megközelíthető területek, és a figyelem lankadása nélkül képes a célterület monitorozására. Megfelelő szenzorokkal felszerelve célzó képessége fölülmúlhatja az emberét. Előreláthatóan a határvédelmi, és járőrözési feladatok megnövekedett szükségessége lesz a fejlesztések motorja. A cél pedig multifunkciós, azaz különféle küldetésekből egyaránt bevethető robotok létrehozása lesz, mely magában foglalja a fegyverek integrációját is¹¹.

A mobilrobotok KKV-szektorban való elterjedésével egyre inkább hétköznapi dologgá válik a robotokkal való találkozás és érintkezés, ami sok új problémát vet fel. Ezekre a problémákra pedig leginkább csak interdiszciplináris tanulmányok adhatnak választ. Fejlesztői oldalról jelentős változást jelent, hogy a kisebb vállalatok nem minden esetben alkalmaznak robotikai szakembereket, az offline programozás pedig jól kalibrált virtuális környezetet igényel¹². Nem elhanyagolható az sem, hogy az üzembe helyezés, vagy az új funkcióra való átállítás ideje alatt a robot nem termel hasznot a vállalatnak, valamint a jelenlegi módszerekkel 400-szor több időt vesz igénybe egy robot beprogramozása, mint elvégezni az adott feladatot¹³. Katonai szempontból viszont, amikor az emberi élet védelme kulcsfontosságú, ezek a pluszköltségek elfogadhatóak, valamint a fejlesztések a multifunkciós robotok irányába mutatnak.

⁹ International Federation of Robotics: Executive Summary World Robotics 2016 Industrial Robots, World Robotics 2016. https://ifr.org/img/uploads/Executive_Summary_WR_Industrial_Robots_20161.pdf. (Letöltés ideje: 2017. 09. 07.)

¹⁰ Ministry of Economy, Trade and Industry (METI): Japan's Robot Strategy was Compiled, 2015, http://www.meti.go.jp/english/press/2015/0123_01.html (Letöltés ideje: 2017. 10. 17.)

¹¹ Technavio Co: Global Military Robots Market 2017-2021, Market Research. Infiniti Research Limited, 2017. <https://www.researchmoz.us/global-military-robots-market-2017-2021-report.html>. (Letöltés ideje: 2017. 10. 20.)

¹² SZIEBIG, Gabor – Peter KORONDI: Effect of Robot Revolution Initiative in Europe – Cooperation possibilities for Japan and Europe, IFAC-PapersOnLine, 11th IFAC Symposium on Robot Control SYROCO 2015, 2015/48. pp. 160–65. <https://doi.org/10.1016/j.ifacol.2015.12.027>. (Letöltés ideje: 2017. 10. 15.)

¹³ THOMESSEN, T. – P.K. SANNÆS – T.K. LIEN: Intuitive robot programming, Proc. 35th International Symposium on Robotics, 2004.

Emellett nem szabad szem elől téveszteni, hogy a robotokat egy eddig nélkülük működő rendszerbe kívánjuk integrálni, amely során alapvető elvárás, hogy az eddigi működés zavartalanul folyhasson tovább. Ehhez a robotokat mind megjelenésükben, mind pedig mozgásukban úgy kell kialakítani, hogy az biztosítsa a nyugodt munkakörnyezetet, az interakciók és kommunikáció pedig természetes és egyszerű legyen.

Robotika a KKV-k szolgálatában

Az ipari robotok telepítése eddig az autóiipari cégek gyáraitra volt jellemző, ahol akár több száz robot is dolgozhat a gyártósoron, előre-, részletesen definiált, különböző komplexitású feladatokon. Ennek során olcsó és magas minőségű, milliós nagyságrendű termékek állíthatók elő.

A KKV-k vagy katonai felhasználás esetében az alkalmazott robotoknak más követelményeknek kell megfelelniük, mivel sokféle terméket viszonylag kis mennyiségben állítanak elő (mert speciális feladatot látnak el). Ez nagy rugalmasságot igényel a gyártó cellától és könnyű átkonfigurálást a termékek között. A legfontosabb feladat az emberi munkaerő kiváltása a monoton, vagy veszélyes munkafolyamatokban, legyen az egy gyártósori alkatrész minőségének ellenőrzése, szállítása, vagy akár egy harcászati megfigyelés, vagy küldetés végrehajtás. Ezáltal a munkakörülmények, a minőség és a produktivitás vagy a hatékonyság is javul. A legnagyobb probléma, hogy ezen gépek klasszikus beüzemelése hosszú időt vesz igénybe, a KKV számára nem kifizetődő robot specialista alkalmazása és a különböző típusú gyártó robotok gyakran nem kompatibilisek egymással.

A kihívást ezáltal a rendszer integrátoroknak kell megoldaniuk, melyre az egyik válasz a rugalmas moduláris keretrendszerek használata. Ilyen például az RT-Middleware¹⁴ vagy a Robot Operation System – ROS¹⁵, ami megoldja a gyors üzembe állítást, csökkenti az átállási időt és lehetőség teremt különböző távfelügyeleti megoldások rendszerszintű alkalmazására.

A rugalmas és intelligens gyártórendszerekben a statikusan telepített (már meglévő, vagy nagyméretű és nehéz) gépek és a többfunkciós mobilrobotok egyszerre tartózkodnak a munkatérben hosszabb ideig, folyamatosan változtatva pozíciójukat. A mobilrobotok továbbá lehetőséget nyújtanak a folyamat kivitelezése¹⁶, és anyagmozgatás egyidejű véghezviteléhez¹⁷ is. Az átkonfigurálható gyártórendszerek

¹⁴ ANDO N. et. al.: RT-middleware: distributed component middleware for RT (robot technology), In 2005 IEEE/RSJ International Conference on Intelligent Robots and Systems, 2005., pp. 3933–3938. <https://doi.org/10.1109/IROS.2005.1545521>. (Letöltés ideje: 2017. 10. 11.)

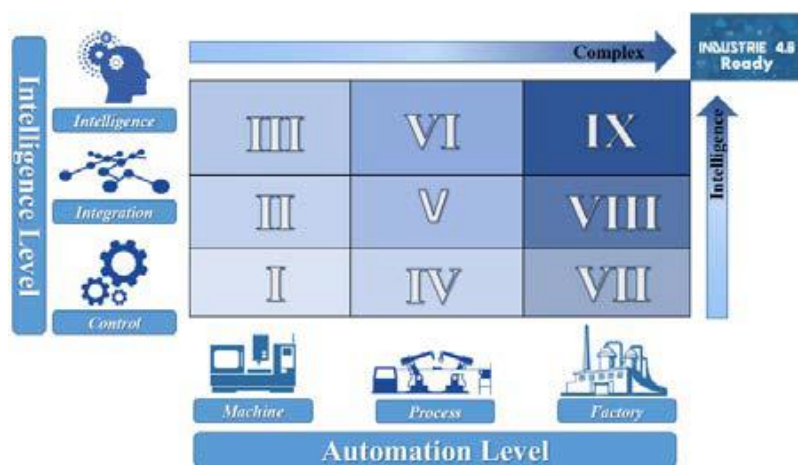
¹⁵ QUIGLEY, Morgan et. al.: ROS: an open-source Robot Operating System, In ICRA workshop on open source software, 3:5. Kobe, 2009. <https://www.willowgarage.com/sites/default/files/icraoss09-ROS.pdf>. (Letöltés ideje: 2017. 10. 15.)

¹⁶ SOMLÓ, K. – G. SZIEBIG: Future role of application of new technologies in small-and medium scale manufacturing systems: Regarding Intelligent and advanced manufacturing systems in northern peripheral area, In: 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), 2017. pp. 1735–1740, <https://doi.org/10.1109/ISIE.2017.8001510>. (Letöltés ideje: 2017. 10. 13.)

¹⁷ BABOLI, Armand et. al.: Intelligent Manufacturing System Configuration and Optimization Considering Mobile Robots, Multi-Functional Machines and Human Operators: New Facilities and Challenge for Industrial Engineering, IFAC-PapersOnLine,

képesek reagálni a piac, vagy műveleti helyzet hirtelen megváltozására és megfelelni az új igényeknek egy adott termékcsaládon belül. Egy ilyen rendszerrel szemben támasztott követelmények a következők: modularitás, integrálható testreszabás, konvertibilitás, skálázhatóság és átláthatóság. Annak ellenére, hogy általában nincs szükség minden funkcióra, a jelenlegi alkalmazások több pontban is kielégítik ezeket a követelményeket azáltal, hogy tartalmazznak CNC gépeket, átalakítható szerszámokat, felügyeleti és szállító rendszereket¹⁸.

Az megmunkáló rendszer összetettsége az alkalmazott intelligencia szintje szerint kategorizálható¹⁹. Az ipar 4.0 fejlesztési trend lényege épp az, hogy egységes rendszerként lehessen kezelni nem csak a különböző gyártási folyamatokat, hanem magát az egész gyárat is, sőt akár azok földrajzilag elkülönülő részeit is össze lehessen kapcsolni. A 4. ábraán bemutatott alkalmazások I szinttől a IX szint felé egyre nagyobb mértékben válnak automatizálttá, rugalmassá és intelligenssé²⁰. A szintek egymásra épülnek, például az intelligens technológia az integráltra épül, ami pedig az automatizálásra. A IX szint képviseli jelenleg a legösszetettebb rendszert, amit Smart Factory-nak is neveznek²¹.



4. ábra: Gyártási folyamatok kategorizálása komplexitás és intelligencia szerint

15th IFAC Symposium on Information Control Problems in Manufacturing, 2015/48. pp. 1912–1917. <https://doi.org/10.1016/j.ifacol.2015.06.366>. (Letöltés ideje: 2017.10. 13.)

¹⁸ KOREN, Y. et. al.: Reconfigurable Manufacturing Systems, CIRP Annals 1999/48. pp. 527–540. [https://doi.org/10.1016/S0007-8506\(07\)63232-6](https://doi.org/10.1016/S0007-8506(07)63232-6). (Letöltés ideje: 2017. 09. 25.)

¹⁹ QIN, Jian – Ying LIU – Roger GROSVENOR: A Categorical Framework of Manufacturing for Industry 4.0 and Beyond, Procedia CIRP, The Sixth International Conference on Changeable, Agile, Reconfigurable and Virtual Production (CARV2016), 2016/52. pp. 173–78. <https://doi.org/10.1016/j.procir.2016.08.005>. (Letöltés ideje: 2017.10. 11.)

²⁰ LEE, Jay: Smart Factory Systems, Informatik-Spektrum 2015/38. pp. 230–235. <https://doi.org/10.1007/s00287-015-0891-z>. (Letöltés ideje: 2017. 10. 03.)

²¹ LEE, Jay – Behrad BAGHERI – Hung-An KAO: A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems, Manufacturing Letters 2015/3. pp. 18–23. <https://doi.org/10.1016/j.mfglet.2014.12.001>. (Letöltés ideje: 2017. 10. 12.); László MONOSTORI et. al.: Cyber-physical systems in manufacturing, CIRP Annals-Manufacturing Technology 2016/65. pp. 621–641. (Letöltés ideje: 2017. 10. 03.)

A rugalmasság magában hordozza, hogy gyors programozási lehetőségek szükségesek, valamint a rendszerrel is komplex interakció lehetőségét kell biztosítani mind a helyi, mind a távoli működtetés terén. Az ezzel kapcsolatos kutatások és eredmények áttekintésére a következő fejezetben térünk ki.

Ember-robot interakció

A szolgáltató robotokkal kapcsolatban felmerülő kérdések közül kulcsfontosságú az ember – robot interakció vizsgálata. Alapvető feladat egy jól definiált kommunikációs csatorna kialakítása a két fél között, amely támogatja a robotok emberközelié válását. Ez történhet a megszokott módon²² (azaz egy külön csatornán keresztül közölve a robottal az aktuális helyzetet leíró paramétereket), vagy megközelíthetjük kognitív módon is a problémát²³. Hasonló elvek alapján célszerű felépíteni az ipari robotok rendszerszintű támogatását kis- és közép vállalatok, valamint a hadipar számára is. Ez alapvetően a rendszerről helyben természetesen elérhető információ (Naturally acquired data – NAD²⁴) közvetítő eszközökön keresztüli továbbításában valósul meg, legyen szó egy távoli felügyeleti rendszerről, vagy éppen a lokális információ átalakításáról. Mivel komplex rendszerek esetén nagymennyiségű információt kell érthető módon továbbítani a humán operátornak, a vizuális és hang alapú érzékelési csatornák mellett kutatások zajlanak a többi érzékszerv, például a tapintás bevonására²⁵. Ez nem csak az érzékszervvel érzékelt direkt információ közvetítést jelenti, hanem az információ áttételét is érzékszervek között, miáltal az multi-modálissá válik. Tapintás során alapvetően a fizikai kontaktus által nyerünk információt az adott tárgyról. Rezgő motorokkal szerelt kesztyűkkel végzett kutatások mutatják, hogy rezgési mintákon keresztül megvalósítható virtuális valóságban is a felületi minőség és anyagmerekési tulajdonságok átadása²⁶, vagy éppen robot konfigurációs és feladatspecifikus információ átadása²⁷. Hatano, Horváth és mtsai 2016-os cikke alapján például rezgési mintákkal egy úgynevezett Fantom-érezkelést fedeztek fel és alkalmaztak pick-and-place robot feladatok során a robot csuklóinak mozgásának

²² F. TAJTI et. al.: CRM TC covering paper – Robotics trends, In: IECON 2013 – 39th Annual Conference of the IEEE Industrial Electronics Society, 2013. pp. 48–53. <https://doi.org/10.1109/IECON.2013.6699110>. (Letöltés ideje: 2017. 10. 15.)

²³ BALAZS, Daniel – Trygve THOMESSEN – Peter KORONDI: Simplified Human-Robot Interaction: Modeling and Evaluation, 2013/34. pp. 199–211. <https://doi.org/10.4173/mic.2013.4.4>. (Letöltés ideje: 2017. 10. 22.)

²⁴ THOMESSEN, Trygve et. al.: Towards Virtual Presence Based on Multimodal Man-Machine Communication: A Remote Operation Support System for Industrial Robots, IFAC-PapersOnLine, 11th IFAC Symposium on Robot Control SYROCO 2015 Salvador, Brazil, 26–28. August 2015, 2015/48. pp. 172–177. <https://doi.org/10.1016/j.ifacol.2015.12.029>. (Letöltés ideje: 2017. 10. 27.)

²⁵ SZIEBIG, G. – P. KORONDI: Remote operation and assistance in human robot interactions with vibrotactile feedback, In: 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), 2017. pp. 1753–1758, <https://doi.org/10.1109/ISIE.2017.8001513>. (Letöltés ideje: 2017. 10. 22.)

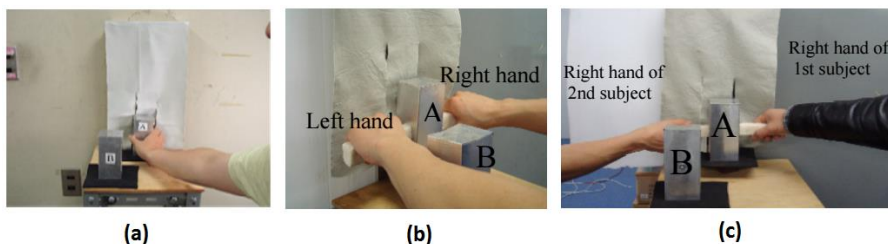
²⁶ GALAMBOS, Péter: Vibrotactile feedback for haptics and telemanipulation: Survey, concept and experiment, Acta Polytechnica Hungarica 2012/9. pp. 41–65. (Letöltés ideje: 2017. 10. 13.)

²⁷ T. HATANO et. al.: A vibrotactile navigation aid for remote operation of an industrial robot, In: 2016 IEEE/SICE International Symposium on System Integration (SII), 2016. pp. 700–705. <https://doi.org/10.1109/SII.2016.7844081>. (Letöltés ideje: 2017. 10. 20.)

visszajelzésére, megfogási és pozicionálási, valamint állapot visszajelzési információk átadására.

Közös munkavégzés során sokszor a siker elengedhetetlen eszköze a szavak nélküli kommunikáció. Ha például partnerünket pozíciójának megváltoztatására szeretnénk rávenni, jelezhetjük ezt egy elhanyagolhatóan kicsi erőbehatással. A behatás intenzitását úgy kell megválasztanunk, hogy a pozícióváltoztatást ne kényszerítse ki, valamint kellemetlen érzetet se keltsen, mindazonáltal egyértelműen érzékelhető legyen a kívánt elmozdulási irány. Ily módon az erőt információközvetítésre használhatjuk fel, és a döntést a tényleges cselekedetről meghagyjuk partnerünknek. Nagy jelentősége van ennek a kommunikációs csatornának abban az esetben, ha közösen szeretnénk vinni egy nehéz csomagot, amely akár hétköznapi-, vagy műveleti és harci helyzetben is előfordulhat. Ilyenkor érzékelnünk kell a partnerünk által kifejtett erők irányát és nagyságát, majd reagálni rájuk, ha nem szeretnénk leejteni terhünket. Sokszor előfordul az az eset is, amikor valamelyik fél hátrafelé kényszerül menni. Ekkor legfőbb információcsatornája a környezetéről (látás) kiesik, és partnerére lesz kénytelen hagyatkozni, akitől a jelenleg tárgyalt módon kap információt.

Ennél a pontnál felmerül az a kérdés, hogy az emberi súlyérzékelés egy robottal segített rendszerrel is megegyezik-e, a nehézségi erő keltette súllyal. Ranham és mtsai cikkükben²⁸ pszichológiai kapcsolatot mutatnak ki szabad súly-, és a robot-rásegítéssel kapcsolatos súly keltette súlyérzet között. A vizsgálathoz egy egyszerű, egy szabadságfokú rendszert terveztek, ahol a három különböző méretű alumíniumdobozba zárt súlyt (tehát megszüntették az összefüggést a látszólagos méret és a tömeg között) lehetett három különböző módon felemelni. Egy kézzel, két kézzel, valamint két eltérő személy egy-egy kézzel együttesen (5. ábra). A rendszer kalibrációját szabadsúlyok keltette súlyérzettel összehasonlítva végezték, a társított súlyokból átlagolással. Az eredmények azt mutatták, hogy a nagyobb objektum méret magasabb csúcserőértékhez vezet a terhelő erőben, valamint ez a csúcserő többszöröse a rendszer által indokolt erőnek. Ennek kiküszöbölésére egy olyan modellt dolgoztak ki, amely külön kezeli a tehetetlenségi erőt a nehézségitől. A vizsgálat közben kimutatták, hogy a tehetetlenségi erő megváltoztatása nem befolyásolja a súlyérzetet. Végül a terhelő erő átlagos csúcserőértékének lecsökkenéséhez a modellben a tehetetlenségi erőt szimbolizáló tömeg (emelés megkezdésének pillanatától kezdődő) exponenciális csökkentése vezetett.



5. ábra: Erő-rásegítéssel rendszer tesztelése fél kézzel (a)-, két kézzel (b)-, és egy-egy kézzel közösen (c) emelve a súlyt

²⁸ S. M. M. RAHMAN et. al.: Controlling a power assist robot for lifting objects considering human's unimanual, bimanual and cooperative weight perception, In: 2010 IEEE International Conference on Robotics and Automation, 2010. pp. 2356–2362. <https://doi.org/10.1109/ROBOT.2010.5509321>. (Letöltés ideje: 2017. 10. 22.)

Egy másik megközelítésben a nyílthurkú vezérlés és a visszacsatolás elemeit kombinálva hoztak létre egy olyan modellt, amely segítségével a robot és az ember képes együttesen elmozdítani egy objektumot a kiindulási pozícióból egy célpozícióba. A problémát három oldalról vizsgálták. Az első a szabályzás (robot betanítása közvetlen mozgás, majd a mozgáslekövetés útján, kétszintes szabályzás, valamint mozgásprimitívek betáplálása a kontrollerbe). A második az emberi interakciók (a feladat precizitása hatással van a mozdulatoknál realizált csillapításra, a merevség integrációjának hatása a modellre, indirekt vizsgálat, amely során az embernek kell alkalmazkodnia a robot mozgásához). A harmadik pedig a gépi tanulás (a GMM – Gaussian Mixture Model alkalmazásával rögzítik a robotkar mozgását, valamint az érzékelt erőket, ezt követően a GMR - Gaussian Mixture Regression segítségével meghatározzák az értékekhez tartozó lehetséges bemenő paramétereket). A robotkar végén egy erőmérő szenzort helyeztek el, modellezése pedig egy rugóból és egy csillapításból állt. A robot betanítása során az objektum áthelyezését a kezdő- és célpozíció között a kísérlet egyik résztvevője oly módon végezte a robottal, hogy a robotkar végét egy betanító személy mozgatta (6. ábra). Ötszöri ismétlés után a robot képes volt a betanító nélkül elvégezni a mozdulatot úgy, hogy minden időpillanatban kiszámolta az elérendő pozíciót és orientációt, valamint az ehhez szükséges gyorsulási és erőkomponenseket. A modell adaptációs képességét mutatja, hogy a robotkar abban az esetben is képes volt elvégezni a mozgást, ha a partnerszemély időről-időre véletlenszerűen módosított az általa kifejtett erő intenzitását. Annak ellenére, hogy ilyen feltételek nem szerepeltek a betanított minták között²⁹.



6. ábra: Robotkar betanítása közös súlymozgatásra

Ezt az elvet felhasználva a rehabilitációs robotok hatékonysága is növelhető. A fizioterápiával kezelhető neuromuszkuláris rendellenességek hatékonyabb rehabilitációja érdekében végzett kutatás keretében létrehoztak egy keretrendszert. Ennek lényege, hogy a betegnek egy robot segítségével közösen kell egy megadott mintának megfelelően falkockákat elhelyeznie a munkaterületen (7. ábra). A

²⁹ ROZO, L. – S. CALINON – D. G. CALDWELL: Learning force and position constraints in human-robot cooperative transportation, In: The 23rd IEEE International Symposium on Robot and Human Interactive Communication, 2014. pp. 619–624.
<https://doi.org/10.1109/ROMAN.2014.6926321>. (Letöltés ideje: 2017. 10. 22.)

rendszer működési elve az, hogy a robot érzékeli a páciens elmozdulását, és segíti végigvinni a mozgást. Emellett a rendszer azt is érzékeli, hogy melyik kockát milyen pozícióba kell mozgatni. Így, ha a páciens rossz irányba akarna mozdulni, a robotkar ellenállást tanúsít, majd korigál. A rehabilitáció során alkalmazott robotok fő előnye az emberrel szemben abban rejlik, hogy a repetitív feladatot a robot időkorlát nélkül, pontosan és fáradhatatlanul tudja végezni, míg az orvos koncentrálna a betegre. Ezek mellett az alkalmazkodás is megjelenik. Mivel a robot érzékeli a beteg által kifejtett erőt, így a páciens mindenkori állapotához tud alkalmazkodni, figyelembe véve a javulást, vagy pedig az elfáradást. Mérnöki szempontból pedig azért előnyös ez a keretrendszer, mert egy nyílt forráskódú rendszerben íródott, és ipari robotokon működtethető, ahogy a cikkben leírt megvalósítás is mutatja³⁰. A gyorsabb és eredményesebb rehabilitáció hadisérülteknél bizonyos esetben döntő fontosságú lehet.



7. ábra: Rehabilitációs gyakorlat végzése robot segítővel

Mobil Robotok pályatervezése zárt térben

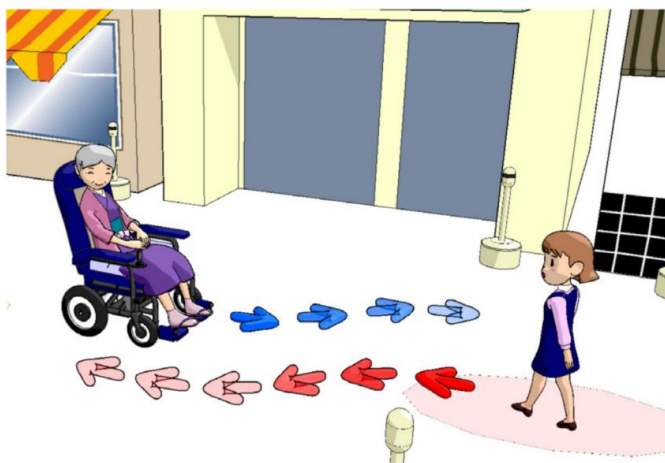
A robotok mozgása, és pályatervezése tiszta mérnöki feladat mindaddig, amíg a robot mozgása egy védett, emberek elől elzárt térre redukálódik. Azonban, ha azt szeretnénk, hogy a szolgáltató robotok emberek között tevékenykedhessenek, ahhoz úgy kell megalkotnunk azokat, hogy ne zavarják a körülöttük lévő embereket hétköznapi tevékenységeikben.

A Morales és munkatársai a 2017-es cikkükben³¹ azt vizsgálják, hogy egy autonóm módon közlekedő kerekesszékek milyen szempontokat kell figyelembe vennie pályatervezése során. Japánban a 6km/h alatti sebességgel mozgó motorikus meghajtású kerekesszék jogilag gyalogosnak minősül, a cél tehát egy olyan pályatervező modell kialakítása, amely hétköznapi szituációkban képes a

³⁰ BADI, Atta – Maryam KARIMI – és Qinggang MENG: Cognitive and Neuromuscular Robotic Rehabilitation Framework. In *Advances in Computational Intelligence Systems, Advances in Intelligent Systems and Computing*. Springer, Cham, 2017. pp. 319–329. https://doi.org/10.1007/978-3-319-46562-3_21. (Letöltés ideje: 2017. 10. 16.)

³¹ MORALES, Yoichi – Takahiro MIYASHITA – Norihiro HAGITA: Social Robotic Wheelchair Centered on Passenger and Pedestrian Comfort, *Robotics and Autonomous Systems* 2017/87. pp. 355–62. <https://doi.org/10.1016/j.robot.2016.09.010>. (Letöltés ideje: 2017. 10. 13.)

gyalogosok közötti navigációra (8. ábra). Ehhez azon alapvető elven kívül, hogy ne ütközzön össze semmilyen akadállyal (beleértve a közlekedésben résztvevő többi gyalogost is), figyelembe kell venni az utas- (mozgáskorlátozott személy), valamint a környező emberek komfortérzetét. Tehát a kerekesszékeknek úgy kell megvalósítani a mozgását, hogy azzal nem csak fizikai, de pszichológiai veszélynek sem teheti ki környezetét. A szembejövőkben kiváltott félelem, vagy az ijedtség éppoly káros lehet az egészségre, mint a kerekesszék használatára szoruló személy állandó szorongása azért, hogy a szükségesnél nagyobb kellemetlenséget okoz embertársainak. A tervezőmérnök feladata tehát kiegészül az ehhez szükséges szempontok vizsgálatával, és figyelembevételével a végső konstrukciónál, ami pedig már túlmutat a tisztán mérnöki nevezhető feladatkörön. A modell megvalósításához megismertek az emberekre jellemző mozgásmintázatokkal, miszerint egy üres úton az emberek közepén szeretnek menni, azonban ha már valaki jön szembe, akkor lehúzódnak az út szélére. Emellett a félrehúzódnál preferált irány a bal, a japán közlekedési viszonyoknak megfelelően. Azt, hogy mennyire kényelmes valami, azt nehéz mérni, ellenben az már könnyebben mérhető, hogy adott szituáció milyen mértékű stresszt vált ki az egyénből. Ezen megfontolás alapján paraméterezhetővé vált, hogy a komfortos mozgás során milyen sebesség-, és gyorsulásértékek engedhetők meg pozíció és helyzetváltoztatáskor és milyen legyen a faltól mért minimális távolság értéke. Végül az előbbi szempontok alapján kialakított modell került összehasonlításra a legrövidebb utat reprezentálóval. Ehhez 15 nő és 15 férfi tesztalanyt választottak és minden résztvevőnek a kerekesszék utasaként, valamint a kerekesszék mellett elhaladó gyalogosként is nyilatkoznuk kellett, hogy mennyire volt számukra komfortos az egymás mellett történő elhaladás a legrövidebb utat, valamint a komfortérzetet figyelembe vevő modell esetén. 1-től 5-ig terjedő skálán 3,96-ra értékelték a kerekesszék utasaként a komfortérzet alapján számoló modellt, míg a legrövidebb út alapján kalkuláló modell esetén az átlagos komfortérzet 2,6 volt. Ugyanezek a számok 4,6 és 3,1 voltak, amikor gyalogosként haladtak el a kerekesszék mellett³². Az első adat reálisabb volna, ha ténylegesen mozgáskorlátozott emberekkel végezték volna el a kísérletet, akikben a kerekesszék használata nem keltett egy szokatlan, kellemetlen érzetet.



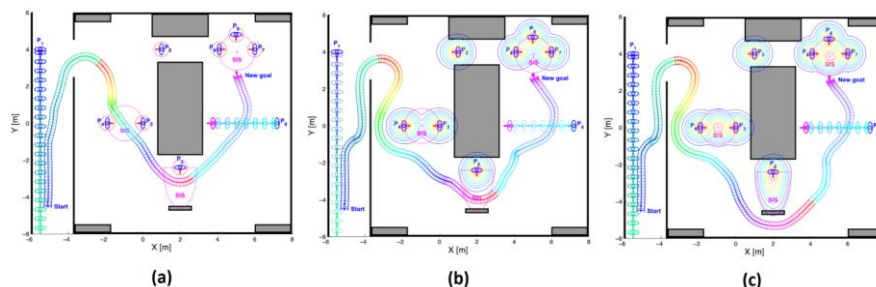
8. ábra: Autonóm mozgású kerekesszék alkalmazása hétköznapi helyzetekre

³² MORALES et. al.: i.m.

Egy szintén 2017-ben megjelent publikációban³³ is pályatervező modell létrehozásával foglalkoznak, azonban itt már egy emberek között, tehát egy dinamikus változó közegben dolgozó robot számára. A modellben egy ember állapotát annak pozíciója, orientációja, mozgása és kezeinek állása határozza meg. Ha a robotra nem csak eszközként tekintünk, hanem az ténylegesen is részt vesz a munkában, akkor a pusztán elkerülésen túl arra is fel kell készítenünk a robotot, hogy egy célszemélyhez, vagy célközösséghez odamenjen. Ilyenkor nem mindegy, hogy a robot milyen távolságra áll meg az embertől, milyen pozícióban, és egyáltalán hogyan közelít az emberhez, vagy embercsoporthoz. A cikkben elsőként egy olyan modell került tesztelésre, amely az embereket egyszerű akadályokként kezeli (9. ábra). Bár a robot ebben az esetben sem ütközött emberrel, egyszer túlságosan megközelített egy mozgásban lévő személyt és semmilyen egyéb társadalmi normát nem vett figyelembe. Megállapítható tehát, hogy amennyiben a robot nem tudja megkülönböztetni az embereket a környező akadályoktól nem garantálható a stresszmentes munkakörnyezet. A modellt ezután kiegészítették egy emberfelismerő rendszerrel, és az egyes emberekhez személyes teret rendeltek (9. ábra). Ebből a szempontból a modellben maga a robot is emberként volt kezelve, és rendelkezett személyes térrel. Ennél a kísérletnél a fizikai biztonság és komfortérzet szempontjából már jóval jobb eredményt értek el. Lényegében, ha két személy egymással való beszélgetésük során elég közel állt egymáshoz, hogy a modellben hozzájuk rendelt személyes terek fedjék egymást, akkor ezt a robot egyetlen elkerülendő objektumnak tekintette és nem zavarta meg őket tevékenységükben. Senkit sem közelített meg olyan mértékben, hogy az ijesztő, vagy zavaró lett volna, azonban még mindig nem vette figyelembe az emberek tevékenységét. Tehát ezzel a modellel még egy fényképező és a megörökíteni kívánt részlet között elhaladva számítaná a robot mozgásának pályáját. A harmadik kísérlet során a modell kiegészítésre került egy érdekes objektumokat is figyelembe vevő rendszerrel (9. ábra). Ennek feladata felismerni, ha egy ember figyelme valamilyen objektumra, vagy akár egy másik személyre összpontosul, és ennek megfelelően az illető személyes terét – vagy az érintett csoportot alkotó egyének személyes tereit – kibővíti egy úgynevezett szociális interakciós térrel. Ennek eredményeként a robot "viselkedése" azon túl, hogy nem okozott sem fizikai, sem pedig pszichikai megrázkódtatást a környezetében dolgozó embereknek a társadalmi normáknak is megfelelővé vált³⁴. Nem elhanyagolható szempont az sem, hogy egy terrorcselekmény elhárítása esetén egy jó pályatervező szoftverrel rendelkező robot pánik-, és a figyelem felkeltését elkerülve tudja megközelíteni a célszemélyeket, vagy éppen a hatástalanítani kívánt robbanószerkezetet.

³³ TRUONG, Xuan-Tung – Trung-Dung NGO: Dynamic Social Zone Based Mobile Robot Navigation for Human Comfortable Safety in Social Environments, *International Journal of Social Robotics* 2016/8, pp. 663–684. <https://doi.org/10.1007/s12369-016-0352-0>. (Letöltés ideje: 2017. 10. 13.)

³⁴ TRUONG – NGO i.m.



9. ábra: Mobil robot pályatervezése célszemély megközelítésére (a) a legrövidebb útvonalon, (b) személyes terek figyelembe vételével, (c) szociális interakciós terek figyelembevételével

Robotok távműködtetése

Egy ismert robotikával foglalkozó publikációban³⁵ egy kutatás eredményét írják le, amelyben egy – az emberi kéz mozgása közben generálódó mioelektromos jelekből, a mozgást rekonstruáló – modellt hoztak létre. A modell célja, hogy később felhasználható legyen exoszkeletonok és protézisek mozgatására, valamint telemanipulációs célokra. A kutatáshoz a NinaPro Database-ből [http://ninapro.hevs.ch/], azaz egy olyan adatbázisból töltöttek le adatokat, amely emberek különféle kéztartás során generálódó sEMG-vel rögzített mioelektromos jeleit tartalmazza mátrixos formában. Ez azt jelenti, hogy a méréshez használt 12 elektróda jelei képzik vektorszerűen a sorokat, míg az oszlopok az adott időpillanatokban reprezentálják ezeket a méréseket. A kísérlet alapja, hogy az sEMG-vel rögzített jelek információt tartalmaznak a mozgás során kialakuló erőről, orientációról és a mozgás típusáról. A mérést megnehezíti, hogy ezzel az eljárással nem lehet tisztán a célizom jeleit mérni, hanem az érzékelően megjelennek a mozgás során aktív környező izmok generálta jelek is. További bonyodalmat okoz, hogy vannak olyan, a mozgás szempontjából meghatározó mélyen elhelyezkedő izmok is, amely jeleinek közvetlen mérése a felszíni EMG-vel nem lehetséges. A cél tehát a mozgásban résztvevő 24 izom jeleinek 12 elektróda segítségével létrehozott vektoraiból az eredeti mozgást rekonstruáló matematikai modell meghatározása volt. Az adatok előkészítése után 4 módszert vizsgáltak, ezek az SVM (Support Vector Machine), ANN (Artificial Neural Networks), K-NN (k-nearest neighbours) és az Ada-RF (Adaboosted RandomForest). Mivel a mérések kiértékelése rámutatott, hogy a mioelektromos jelek segítségével betanított modell az egyénre jellemző információkat tartalmaz, így egy olyan módszert kellett találni, amely gyors betanítást és magas pontosságot tesz lehetővé. Ezt pedig a K-NN módszer tudta reprezentálni, 3 ismétlésszám mellett (a mérésük alapján a pontosság 95,39%, míg 4 ismétlés esetén 97,00%). A modell robusztusságát mutatja, hogy elvégezték a méréseket olyan emberekkel is, akiknek az alkarjuk különféle mértékben amputálásra került, és a mintavételek számát kétszeresére növelve a rekonstruálhatóság a hiány mértékétől függően 90% fölötti pontosságot mutatott, bár ebben az esetben a modell kiértékelési ideje is a duplájára nőtt. A 10. ábra a

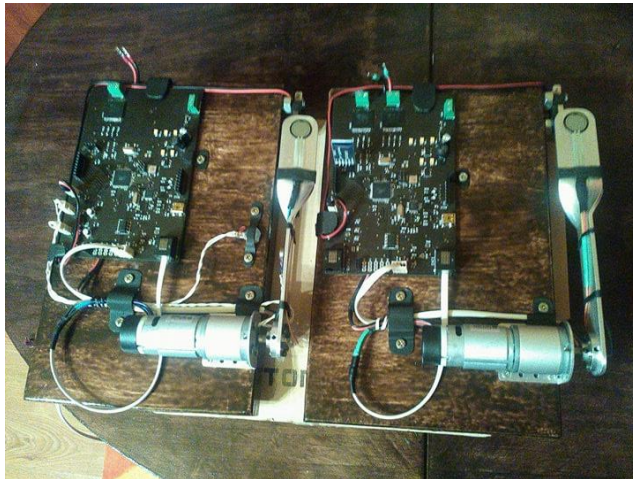
³⁵ WEI, Jiefei – Qinggang MENG – Atta BADI: Classification of Human Hand Movements Using Surface EMG for Myoelectric Control, In: Advances in Computational Intelligence Systems, Advances in Intelligent Systems and Computing. Springer, Cham, 2017. pp. 331–339. https://doi.org/10.1007/978-3-319-46562-3_22. (Letöltés ideje: 2017. 10. 15.

kísérletben résztvevő amputált alanyok által produkált eredményeket mutatja be, ahol az első sor az amputációt követően megmaradt alkar százalékosan becsült mértékét tartalmazza (Remaining Forearm), a második sor 400 mintavétel esetén (400 rows)-, a harmadik pedig 800 mintavétel esetén (800 rows) mutatja a pontosságot. Ezzel a módszerrel természetesebben mozgatható művégtagokat lehetne létrehozni, amely többek között sok hadisérült életkörülményeinek javítását tenné lehetővé.



10. ábra: Mozgás rekonstrukciója mioelektromos jelekből amputált személyek esetén

A Budapesti Műszaki és Gazdaságtudományi Egyetem MOGI tanszékén egy jelenleg is zajló kutatás témája annak vizsgálata, hogy egy vezérlőkar segítségével hogyan lehet erő-visszacsatolás nélkül egy távoli szolgálatszösz (slave) adott nagyságú és irányú erőkifejtését biztosítani. A kutatás célja, hogy megvizsgálja, és rangsorolja azokat az érzékelési lehetőségeket, melyek az erő közvetlen érzékelésén túl segítségünkre lehetnek egy telemanipulációs feladat során (11. ábra). Ez jelentőséggel bírhat ember által közvetlenül vezérelt harci robotok irányítása esetén, egy távolról végzett műtétnél, vagy más olyan feladatnál, ahol az ember által történő megközelítés nem lenne megoldható, vagy veszélyes lenne.

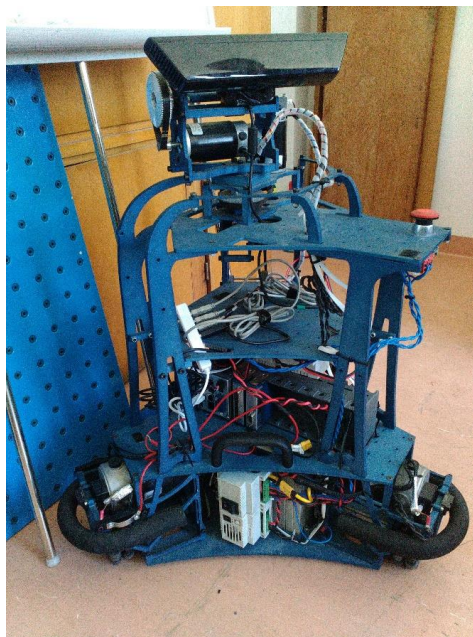


11. ábra: Telemanipulációs mester és szolgálatszösz, az érzékelési lehetőségek vizsgálatára

Etorobotika

Az etorobotika a robotok viselkedését vizsgáló tudományterület, melynek az emberek mindennapjait segítő, szolgáltató robotoknál lesz a legnagyobb jelentősége, de nem elhanyagolható a hadi alkalmazás során sem, ahol fontos a feltűnésmentes feladat-végrehajtás. A szolgáltató robotok esetében nem elégséges egy előreprogramozott mozdulatsor végrehajtása, mint például egy ipari robot esetében, hanem kulcsfontosságú, hogy a változó körülményekre reagálni tudjon. Döntéseit pedig úgy kell meghoznia, hogy viselkedése illeszkedjen az emberi környezet elvárásaihoz. Ehhez elengedhetetlen, hogy kommunikálni tudjon a környezetével és viszonylag gyorsan megértse, hogy mi a feladata. Az, hogy a robot milyen mértékű kommunikációra képes egy meghatározó viselkedésforma, mely befolyással lehet a robot integrációjára a mindennapi életünkbe. Amennyiben a robot csak korlátozott számú kommunikációs mintával rendelkezik, akkor az újdonság-érzet elmúltával a robot kikerül majd az érdeklődés középpontjából. Így ennek a területnek a kutatása nagy előrelépést jelentene az etorobotikában³⁶.

Ha a kiszolgáló robotok aktívan részvevő segítőként válnak részeseivé az emberek mindennapjainak, akkor kialakulhat egyfajta érzelmi kötődés robot és ember között. Ez a kötődés elősegítheti a robotok társadalmi elfogadottságát is. Az Eötvös Lóránd Tudomány Egyetem, Etológia Tanszékének kutatócsoportja az etorobotok viselkedését, és ezzel a „családokban betöltött szerepüket” is egy kutyáéhoz hasonlóan határozzák meg³⁷.



12. ábra: MOGI ETHON

³⁶ KORONDI, Péter et. al.: Etho-robotics: What kind of behaviour can we learn from the animals?, IFAC-PapersOnLine 2015/48. pp. 244–255. (Letöltés ideje: 2017. 10. 12.)

³⁷ FARAGÓ, Tamás et. al.: Social behaviours in dog-owner interactions can serve as a model for designing social robots, Interaction Studies 2014/15. pp. 143–172. <https://doi.org/10.1075/is.15.2.01far>. (Letöltés ideje: 2017. 10. 11.)

A házakban történő manőverezéshez a – gyári környezethez képest szűkebb terek miatt – nagy hangsúly kerül mind a robot hajtásrendszerének kialakítására, mind pedig a pályatervezésre. A cikkben tárgyalt, Budapesti Műszaki és Gazdaságtudományi Egyetem MOGI Tanszékén kutatási céllal létrehozott MOGI-ETHON (12. ábra) névre keresztelt robot esetében a holonomikus hajtásrendszer került kiválasztásra, melyhez pályatervező algoritmus is készült. A holonomikus hajtás egy speciális kerék használatán alapul, melynél a kerék futófelülete mentén oly módon helyezkednek el görgők, hogy lehetővé tegyék a kerék forgásirányra merőleges elmozdulását (13. ábra). Három ilyen kerék megfelelő elhelyezésével megvalósítható, hogy a robot mozgásának irányvektora – az emberek és állatok többségéhez hasonlóan – eltérő irányba mutathasson, mint amerre a robot eleje mutat ("~néz").



13. ábra: OMNIWHEEL

Katonai célú robotizálás

A robotok civil környezetben történő biztonságos alkalmazása egy új szintre emeli a katonai feladatokra történő alkalmazásukat is. Amíg emberi intelligenciát igénylő feladatokban teljesítményük elmarad, addig sok esetben jóval felülmúlják a humán katonák lehetőségeit. Az egyik, talán legfontosabb szempont, hogy az emberi élet felbecsülhetetlen értékével szemben a modern gyártási technológiáknak köszönhetően a robotok gyártási költsége igen kedvező. Emellett a modern elektronika és számítástechnika alkalmazásával pontosságuk, számítási kapacitásuk, adattárolásuk és döntési sebességük többszörösen felülmúlja az emberi képességeket. Fontos szempont, hogy olyan helyeken is bevethetőek, ahol a környezeti feltételek alig, vagy egyáltalán nem alkalmasak emberek számára³⁸. Bizonyos életveszélyes műveleteknél az emberi jelenlét tökéletesen kiváltható robotok alkalmazásával. Ha például egy felderítési feladatot kell végrehajtani ellenséges területen, egy UAV elvégezheti azt anélkül, hogy egy felderítő katona elfogását kockáztatnánk. Egy robbanószerkezet hatástalanítása esetén első lépésként szintén egy UAV segítségével megtörténhet a lokalizáció, és a szükséges

³⁸ SZEGEDI, Péter– Péter KORONVÁRY– Bertold BÉKÉSI: The use of Robots in Military Operations, Scientific Research and Education in the Air Force 2017/19, pp. 221–230. <https://doi.org/10.19062/2247-3173.2017.19.1.25>. (Letöltés ideje: 2017. 10. 15.)

információk összegyűjtése (robbanószerkezet típusa, időzítő, vagy távműködtetés esetén a szükséges személyek lokalizálása stb.). A felderítőrobotba már eleve integrálható egy hatalmas adatbázis, amely alkalmas a bomba azonosítására. Itt fontos megjegyezni azt is, hogy egy robbanószerkezetek hatástalanítására specializálódott szakember betanítása hosszú időbe telik, míg egy robot felprogramozása egy tetszőlegesen nagy és részletes adatbázissal egy pillanat. Ezt követően egy tűzszerész nehézrobot (14. ábra) tetszőlegesen modifikálható, felkészíthető a célfeladatra. Szükség esetén a speciális multifunkciós fűróeszköz, röntgenkeret, disruptor egység és vegyi detektorok kiegészíthetők egy frekvenciazavaró eszközzel (jammer), mellyel megakadályozható a robbanószerkezet távolról történő működésbe hozása³⁹.



14. ábra: KNIGHT tűzszerész nehézrobot

Emellett léteznek még a felderítés mellett célpont megsemmisítésére alkalmas drónok is, melyekbe nagy hatótávú szenzorok és precíziós fegyverek kerültek integrálásra. Ilyen például a General Atomics MQ-9 Reaper vagy a Predator XP⁴⁰. Mivel ez a drón inkább hasonlít egy kisebb fajta repülőgépre, így felszerelhető akár lézer vezérelt bombákkal, vagy levegő-föld rakétákkal⁴¹. Az 1979-ben tervezett Goalkeeper⁴² modernizált változata egy teljesen automatizált fegyverrendszert valósít meg. Fejlett szenzorjainak köszönhetően biztosítja a hadihajók légvédelmét mind légi járművek, mind pedig rakéták ellen, valamint a vízfelszínen közlekedő járművek észlelésére és megsemmisítésére is alkalmas.

³⁹ KOVÁCS (2014.) i.m.

⁴⁰ General Atomics: Aircraft Platforms, General Atomics Aeronautical Systems Inc. <http://www.ga-asi.com/aircraft-platforms>. (Letöltés ideje: 2017. 10. 27.)

⁴¹ SZEGEDI et. al.: i.m.

⁴² Thales Group: Goalkeeper – close-in weapon system, <https://www.thalesgroup.com/en/goalkeeper-close-weapon-system>. (Letöltés ideje: 2017. 10. 27.)

A műveleti területeken nem csak a felderítésre és megsemmisítésre alkalmas robotoknak van létjogosultsága. A BigDog⁴³ névre hallgató robot egy olyan speciális teherszállító, mely alkalmas 150 kg teher szállítására akár nehéz terepen (sziklás, csúszós, sáros) is, ezzel támogatva a földi egységeket. Az integrált számítógépes egység lehetővé teszi a távolról történő irányítást.

A robotok civil szférában történő elterjedésének fontos kihatásai lehetnek a hadi iparban alkalmazott robotokra. Egyrészt, hogy ha az emberek hozzászoknak ahhoz, hogy robotok veszik őket körül, akkor viszonylag feltűnésmentesen lehet végrehajtani a hadi műveleteket civilekkel teli környezetben. Másrészt pedig az, hogy amíg a hadiparban a hatékonyságra kerül a hangsúly, addig a civil szférában legalább ennyire fontos a kényelem, a barátságos és esztétikus megjelenés. További nagyon fontos szempont az is, hogy a civil szférában végzett kutatások általában publikusak – szemben a hadipar kutatásaival -, így egy globális, egymásra épülő kutatási hullám jöhet létre, amely minden terület számára hasznos innovációkat eredményezhet.

Intelligens terek

A számítástechnikai eszközök fejlődése mára lehetővé tette az úgynevezett intelligens terek alkalmazását is. Ezek kiterjedt szenzorrendszer segítségével megfigyelés alá vont területek, amelyekben az egyes szenzorok adatait kisebb feldolgozó egységek elemzik és osztják meg egy közös hálózaton. (Az alkalmazott szenzorok sokfélék lehetnek, mint például vizuális, audio, vagy heptikus.) Egy ilyen szenzorból, processzorból és kommunikációs interfészből álló egységet DIND-nek, azaz Elosztott Intelligenciájú Hálózati Eszköznek nevezünk. Ezen túlmenően az intelligens tereknek rendelkezniük kell passzív vagy aktív aktuátorokkal is. Passzív aktuátor alatt egy kijelzőt, aktív alatt pedig például egy robotot érthetünk. Az intelligens tér tehát egy olyan szenzorokat, aktuátorokat és feldolgozókat magába foglaló hálózat, mely képes a benne zajló események érzékelésére, elemzésére, valamint reagálni is tud azokra.

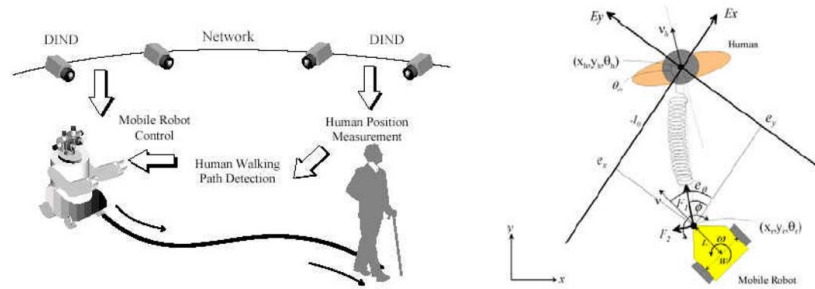
Az intelligens terek alkalmazásával a robottechnikában egyfajta paradigmaváltás valósul meg. Az eddigi nézet szerint ugyanis az volt a cél, hogy az egyes robotok önálló egységként létezzenek, tehát saját szenzorrendszerrel legyenek ellátva, melynek adatait a robot saját maga dolgozza fel és ezek alapján reagáljon a külvilágra. Az új rendszer szerint viszont az egyes robotok viselkedését a komplett hálózati rendszer határozza meg, és hangolja össze, amelybe természetesen beletartoznak az adott robot érzékelői által összegyűjtött adatok is.

Korondi Péter írásában⁴⁴ elemzésre kerül, hogy miként valósulhat meg egy ember robot által történő követése az intelligens térben. Ehhez mindenképp az emberek felismerését kell biztosítani, amely a fej és a kezek állásának meghatározásával történik, a bőrszint felismerő algoritmusok segítségével. Ezen kívül a rendszernek fel kell ismernie a térben található, vagy abba belépő akadályokat is, melyek matematikailag potenciál-függvényekkel definiálhatóak, valamint ismernie kell

⁴³ Boston Dynamics: BigDog, <https://www.bostondynamics.com/bigdog>. (Letöltés ideje: 2017. 10. 27.)

⁴⁴ KORONDI, Péter: Intelligens Tér, paradigma váltás az emberek tájékoztatásában és kiszolgálásában című előadás, Országos Térinformatikai Konferencia, Szolnok, 2004. <http://www.otk.hu/cd04/plenaris/Korondi%20P%C3%A9ter.htm#top>. (Letöltés ideje: 2017. 10. 04.)

egyfajta kitérésí stratégiát is az akadályok elkerülésére, amelyhez kognitív szempontok figyelembevétele szükséges. Végül a robot úgy fogja követni az embert, mintha egy láthatatlan rugóval lennének egymással összekötve (15. ábra), azaz hirtelen sebességváltozásokra késleltetetten fog reagálni.



15. ábra: Ember követése robot által (bal) a robot követi az embert az intelligens térben (jobb) a követés modellje

Intelligens terek segítségével biztosítani lehetne egy olyan környezetet, melyben robotok segítik az emberek munkavégzését, valamint extrém esetekben -, mint például tűz, betörés, vagy terrorcselekmény – a rendelkezésre álló pluszinformációk segítségével biztosíthatnák a környező emberek testi épségét (optimális útvonalon való terelés).

Összegzés

Írásunkban a robotpiac fejlődési irányvonalát tekintettük át, melynek középpontjában az eddigi ipari és hadi robotok helyett előreláthatólag a szolgáltató szektor fog kerülni. A szolgáltató robotok olyan (akár személyes felhasználású) mobil célrobotok, melyeknek tevékenységüket hétköznapi környezetben, emberek között kell végrehajtaniuk. Ez egy rendkívül változékony és inger gazdag környezet, mely teljesen új kihívásokat jelent a robotok tervezésében. Ezekre a kihívásokra egyedül interdiszciplináris kutatások jelenthetnek választ. Ennek jegyében áttekintettünk néhány aktuális kutatást, amelyek a szolgáltató robotok teremtette új elvárások, valamint a katonai célú robotokkal kapcsolatos főbb témákra irányultak. Ezek a humán-robot interakción belül a közös munkavégzés, kommunikáció és az érzékelést tárgyalták.

A mobil robotok pályatervezésén belül olyan modellekről esett szó, amelyek figyelembe veszik az „élő” környezetet, miközben a cél egy adott pozíció elérése, vagy akár egy célcsoport megközelítése. Ennek kiemelkedő szerepe lehet terror-elhárítási, valamint műveleti területen végzett feladatok végrehajtásánál. A robotok távműködtetésének keretében a mozdulatok felismerésére, valamint a különböző típusú érzékelések vizsgálatára koncentráltunk az emberközeli, minél természetesebb irányítás megvalósításáért. Majd az etorobotika témakörében a robotok azon tulajdonságaira koncentráltunk, amelyek segíteni tudják a robotok „beilleszkedését” a társadalmunkba.

A látszat ellenére ennek is kulcsfontosságú szerepe lehet a terrorrelhárításban, hiszen ha feltűnés nélkül szeretnénk eljuttatni egy robotot a céljához, ahhoz el kell érniük, hogy a környező civileknek a robot jelenléte természetes legyen. Ezt követően a kifejezetten harcászati célra tervezett robotokkal foglalkoztunk, kiemelve a robotok

előnyeit az emberrel szemben bizonyos feladatok esetén. Valamint rámutattunk a civilszféra kutatásainak hasznosságára a hadipar szemszögéből.

Végül pedig az intelligens terekkel egy olyan keretrendszert mutattunk be, amely alkalmas az egyes robotok, mint egyének rendszerbe foglalására és adott helyekre vonatkozó speciális szabályok közlésére a robotokkal (például: könyvtárban lassú közlekedés és csendes üzemmód, művelési területeken az aktuális szabályok vagy esetleg egy terrorcselekmény esetén a környező civilek magántulajdonában álló robotok feletti irányítás átvétele).

Felhasznált irodalom:

- ANDO, N. – T. SUEHIRO – K. KITAGAKI – T. KOTOKU – Woo-Keun YOON: RT-middleware: distributed component middleware for RT (robot technology), In 2005 IEEE/RSJ International Conference on Intelligent Robots and Systems, 2005., pp. 3933–3938. <https://doi.org/10.1109/IROS.2005.1545521>. (Letöltés ideje: 2017. 10. 11.)
- BABOLI, Armand – Jun OKAMOTO – Marcos S. G. TSUZUKI – Thiago C. MARTINS – Paulo E. MIYAGI – Fabrício JUNQUEIRA: Intelligent Manufacturing System Configuration and Optimization Considering Mobile Robots, Multi-Functional Machines and Human Operators: New Facilities and Challenge for Industrial Engineering, IFAC-PapersOnLine, 15th IFAC Symposium on Information Control Problems in Manufacturing, 2015/48. pp. 1912–1917. <https://doi.org/10.1016/j.ifacol.2015.06.366>. (Letöltés ideje: 2017.10. 13.)
- BADII, Atta – Maryam KARIMI – és Qinggang MENG: Cognitive and Neuromuscular Robotic Rehabilitation Framework. In Advances in Computational Intelligence Systems, Advances in Intelligent Systems and Computing. Springer, Cham, 2017. pp. 319–329. https://doi.org/10.1007/978-3-319-46562-3_21. (Letöltés ideje: 2017. 10. 16.)
- BÉKÉSI, Bertold– Péter SZEGEDI: Napjaink fegyverrendszer fejlesztési trendjei. *Economica* (1585-6216) 2015/8. pp. 158-168., <http://eds.b.ebscohost.com/abstract?site=eds&scope=site&jrnl=15856216&AN=113875035&h=3B8JwiRgkvTYGCoSfNF42C%2fjeNzWyqGaPty1nu4z5fe9EIdVOsIKwrnfEoW1qja1oLcRoHYWD1ZQIM7nV1HBCQ%3d%3d&crl=c&resultLocal=ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d15856216%26AN%3d113875035>. (Letöltés ideje: 2017. 09. 27.)
- Boston Dynamics: BigDog, <https://www.bostondynamics.com/bigdog>. (Letöltés ideje: 2017. 10. 27.)
- BALAZS, Daniel – Trygve THOMESSEN – Peter KORONDI: Simplified Human-Robot Interaction: Modeling and Evaluation, 2013/34. pp. 199–211. <https://doi.org/10.4173/mic.2013.4.4>. (Letöltés ideje: 2017. 10. 22.)
- FARAGÓ, Tamás– Ádám MIKLÓSI – Beáta KORCSOK – Judit SZÁRAZ – Márta GÁCS: Social behaviours in dog-owner interactions can serve as a model for designing social robots, *Interaction Studies* 2014/15. pp. 143–172. <https://doi.org/10.1075/is.15.2.01far>. (Letöltés ideje: 2017. 10. 11.)

- GALAMBOS, Péter: Vibrotactile feedback for haptics and telemanipulation: Survey, concept and experiment, *Acta Polytechnica Hungarica* 2012/9. pp. 41–65. (Letöltés ideje: 2017. 10. 13.)
- General Atomics: Aircraft Platforms, General Atomics Aeronautical Systems Inc. <http://www.ga-asi.com/aircraft-platforms>. (Letöltés ideje: 2017. 10. 27.)
- HATANO, T. – C. M. HORVATH – T. THOMESSEN – M. NIITSUMA: A vibrotactile navigation aid for remote operation of an industrial robot, In: 2016 IEEE/SICE International Symposium on System Integration (SII), 2016. pp. 700–705. <https://doi.org/10.1109/SII.2016.7844081>. (Letöltés ideje: 2017. 10. 20.)
- IFR: World Robotics Survey, IFR International Federation of Robotics, <https://ifr.org/ifr-press-releases/news/world-robotics-survey-service-robots-are-conquering-the-world->. (Letöltés ideje: 2017. 09. 07.)
- International Federation of Robotics: Executive Summary World Robotics 2016 Industrial Robots, World Robotics 2016. https://ifr.org/img/uploads/Executive_Summary_WR_Industrial_Robots_20161.pdf. (Letöltés ideje: 2017. 09. 07.)
- KOREN, Y. – U. HEISEL – F. JOVANE – T. MORIWAKI – G. PRITSCHOW – G. ULSOY – H. VAN BRUSSEL: Reconfigurable Manufacturing Systems, *CIRP Annals* 1999/48. pp. 527–540. [https://doi.org/10.1016/S0007-8506\(07\)63232-6](https://doi.org/10.1016/S0007-8506(07)63232-6). (Letöltés ideje: 2017. 09. 25.)
- KORONDI Péter: Intelligens Tér, paradigma váltás az emberek tájékoztatásában és kiszolgálásában című előadás, Országos Térinformatikai Konferencia, Szolnok, 2004. <http://www.otk.hu/cd04/plenaris/Korondi%20P%C3%A9ter.htm#top>. (Letöltés ideje: 2017. 10. 04.)
- KORONDI, Péter , Beáta KORCSOK, Szilveszter KOVÁCS, és Mihoko NIITSUMA: Etho-robotics: What kind of behaviour can we learn from the animals?, *IFAC-PapersOnLine* 2015/48. pp. 244–255. (Letöltés ideje: 2017. 10. 12.)
- KOVÁCS Zoltán Tibor: Az improvizált robbanóeszközök elleni védelem elvei, módszerei és eljárásai, 2014. <http://real.mtak.hu/16086/1/Improviz%C3%A1lt%20robban%C3%B3eszk%C3%B6z%C3%B6k%20elleni%20v%C3%A9delem%20elvei%20m%C3%B3dszerei%20%20%20elj%C3%A1r%C3%A1sai.pdf> (Letöltés ideje: 2017. 09. 27.)
- LEE, Jay: Smart Factory Systems, *Informatik-Spektrum* 2015/38. pp. 230–235. <https://doi.org/10.1007/s00287-015-0891-z>. (Letöltés ideje: 2017. 10. 03.)
- LEE, Jay – Behrad BAGHERI – Hung-An KAO: A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems, *Manufacturing Letters* 2015/3. pp. 18–23. <https://doi.org/10.1016/j.mfglet.2014.12.001>. (Letöltés ideje: 2017. 10. 12.)
- Ministry of Economics and Trade (METI): 2035nen ni muketa robotto sangyou no shourai shijou yosoku (Market forecast of robot industry in 2035). Ministry of Economics and Trade (METI), 2010. <http://www.meti.go.jp/press/20100423003/20100423003-2.pdf>. (Letöltés ideje: 2017. 10. 17.)

- Ministry of Economy, Trade and Industry (METI): Japan's Robot Strategy was Compiled, 2015, http://www.meti.go.jp/english/press/2015/0123_01.html (Letöltés ideje: 2017. 10. 17.)
- Ministry of Economy, Trade and Industry (METI): Announcement of the Results of a Trend Survey on the Robot Industry Market Japan Maintains the World's Top Market Share and the Chinese Market is Rapidly Growing, 2013. http://www.meti.go.jp/english/press/2013/0718_02.html. (Letöltés ideje: 2017. 09. 17.)
- MONOSTORI, László – Botond KÁDÁR – T. BAUERNHANSL – S. KONDOH – S. KUMARA – G. REINHART – O. SAUER – G. SCHUH – W. SIHN – és K. UEDA: Cyber-physical systems in manufacturing, *CIRP Annals-Manufacturing Technology* 2016/65. pp. 621–641. (Letöltés ideje: 2017. 10. 03.)
- MORALES, Yoichi – Takahiro MIYASHITA – Norihiro HAGITA: Social Robotic Wheelchair Centered on Passenger and Pedestrian Comfort, *Robotics and Autonomous Systems* 2017/87. pp. 355–62. <https://doi.org/10.1016/j.robot.2016.09.010>. (Letöltés ideje: 2017. 10. 13.)
- QIN, Jian – Ying LIU – Roger GROSVENOR: A Categorical Framework of Manufacturing for Industry 4.0 and Beyond, *Procedia CIRP, The Sixth International Conference on Changeable, Agile, Reconfigurable and Virtual Production (CARV2016)*, 2016/52. pp. 173–78. <https://doi.org/10.1016/j.procir.2016.08.005>. (Letöltés ideje: 2017.10. 11.)
- QUIGLEY, Morgan – Ken CONLEY – Brian GERKEY – Josh FAUST – Tully FOOTE – Jeremy LEIBS – Rob WHEELER – Andrew Y. NG: ROS: an open-source Robot Operating System, In *ICRA workshop on open source software*, 3:5. Kobe, 2009. <https://www.willowgarage.com/sites/default/files/icraoss09-ROS.pdf>. (Letöltés ideje: 2017. 10. 15.)
- RAHMAN, S. M. M. – R. IKEURA – M. NOBE – H. SAWAI: Controlling a power assist robot for lifting objects considering human's unimanual, bimanual and cooperative weight perception, In: *2010 IEEE International Conference on Robotics and Automation*, 2010. pp. 2356–2362. <https://doi.org/10.1109/ROBOT.2010.5509321>. (Letöltés ideje: 2017. 10. 22.)
- ROZO, L. – S. CALINON – D. G. CALDWELL: Learning force and position constraints in human-robot cooperative transportation, In: *The 23rd IEEE International Symposium on Robot and Human Interactive Communication*, 2014. pp. 619–624. <https://doi.org/10.1109/ROMAN.2014.6926321>. (Letöltés ideje: 2017. 10. 22.)
- SANDER, Alison – Meldon Wolfgang: The rise of robotics, *The Boston Consulting Group*, 2014/27. http://img-stg.bcg.com/The_Rise_of_Robotics_Aug_2014_tcm9-82495.pdf. (Letöltés ideje: 2017. 10. 27.)
- SOMLÓ, K. – G. SZIEBIG: Future role of application of new technologies in small- and medium scale manufacturing systems: Regarding Intelligent and advanced manufacturing systems in northern peripheral area, In: *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, 2017. pp. 1735–1740, <https://doi.org/10.1109/ISIE.2017.8001510>. (Letöltés ideje: 2017. 10. 13.)

- SZEGEDI Péter – KORONVÁRY Péter – BÉKÉSI Bertold: The use of Robots in Military Operations, Scientific Research and Education in the Air Force 2017/19. pp. 221–230. <https://doi.org/10.19062/2247-3173.2017.19.1.25>. (Letöltés ideje: 2017. 10. 15.)
- SZIEBIG, G. – P. KORONDI: Remote operation and assistance in human robot interactions with vibrotactile feedback, In: 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), 2017. pp. 1753–1758, <https://doi.org/10.1109/ISIE.2017.8001513>. (Letöltés ideje: 2017. 10. 22.)
- SZIEBIG, Gabor – Peter KORONDI: Effect of Robot Revolution Initiative in Europe – Cooperation possibilities for Japan and Europe, IFAC-PapersOnLine, 11th IFAC Symposium on Robot Control SYROCO 2015, 2015/48. pp. 160–65. <https://doi.org/10.1016/j.ifacol.2015.12.027>. (Letöltés ideje: 2017. 10. 15.)
- Szn.: Japan's Robot Strategy was Compiled, 2015. http://www.meti.go.jp/english/press/2015/0123_01.html. (Letöltés ideje: 2017. 10. 27.)
- TAJTI, F. – G. SZAYER – B. KOVÁCS – B. DÁNIEL – P. KORONDI: CRM TC covering paper – Robotics trends, In: IECON 2013 – 39th Annual Conference of the IEEE Industrial Electronics Society, 2013. pp. 48–53. <https://doi.org/10.1109/IECON.2013.6699110>. (Letöltés ideje: 2017. 10. 15.)
- Technavio Co: Global Military Robots Market 2017-2021, Market Research. Infiniti Research Limited, 2017. <https://www.researchmoz.us/global-military-robots-market-2017-2021-report.html>. (Letöltés ideje: 2017. 10. 20.)
- Thales Group: Goalkeeper – close-in weapon system, <https://www.thalesgroup.com/en/goalkeeper-close-weapon-system>. (Letöltés ideje: 2017. 10. 27.)
- THOMESSEN, T. – P.K. SANNÆS – T.K. LIEN: Intuitive robot programming, Proc. 35th International Symposium on Robotics, 2004.
- THOMESSEN, Trygve – Mihoko NIITSUMA – Keita SUZUKI – Takashi HATANO – Hideki HASHIMOTO: Towards Virtual Presence Based on Multimodal Man-Machine Communication: A Remote Operation Support System for Industrial Robots, IFAC-PapersOnLine, 11th IFAC Symposium on Robot Control SYROCO 2015 Salvador, Brazil, 26–28. August 2015, 2015/48. pp. 172–177. <https://doi.org/10.1016/j.ifacol.2015.12.029>. (Letöltés ideje: 2017. 10. 27.)
- TRUONG, Xuan-Tung – Trung-Dung NGO: Dynamic Social Zone Based Mobile Robot Navigation for Human Comfortable Safety in Social Environments, International Journal of Social Robotics 2016/8, pp. 663–684. <https://doi.org/10.1007/s12369-016-0352-0>. (Letöltés ideje: 2017. 10. 13.)
- WEI, Jiefei – Qinggang MENG – Atta BADI: Classification of Human Hand Movements Using Surface EMG for Myoelectric Control, In: Advances in Computational Intelligence Systems, Advances in Intelligent Systems and Computing. Springer, Cham, 2017. pp. 331–339. https://doi.org/10.1007/978-3-319-46562-3_22. (Letöltés ideje: 2017. 10. 15.)

KOVÁCS KRISZTIÁN

ALDRICH HAZEN AMES TÖRTÉNETE I.

Bevezetés

A XX. század második felében, a hidegháború időszakában a kétpólusú világrend szereplőinek viszonyát súlyos feszültség jellemezte, amelyben az érdekérvényesítés egyik fontos eszköze volt a titkosszolgálatok aktív, támadólagos alkalmazása. Ennek megmutatkozása az a számos kémügy, amelyeket – többé-kevésbé – megismerhettünk, így bepillantást nyerhettünk az elhárítás és hírszerzés eljárásrendjébe, tevékenységébe.

Ezek az esetek szakmatörténeti szempontból is jelentőséggel bírnak, mert a kiélezett biztonságpolitikai környezetben – amely minden esetben alapvető meghatározója a titkosszolgálati tevékenységnek – mutatják be a kémkedés és kémelhárítás lehetőségeit és korlátait, illetve az elhárító és hírszerző szolgálatok működését, viszonyát.

A híres kém-történetek közül Aldrich Hazen Ames esetét mutatom be, aki 1994-ig az amerikai Central Intelligence Agency (CIA, Központi Hírszerző Ügynökség) állományában szolgált, de a 80'-as évek közepén önként jelentkezett a szovjeteknél, hogy számukra kémkedjen. Árulása során számos szovjet/ orosz ügynököt buktatott le, akik többségét ki is végezték. Történetével oly sok könyv, dolgozat és film foglalkozott, hogy vélhetőleg annak már minden részlete ismert, ezért tanulmányomban nem is az újabb részletek feltárására, hanem a megismerhető események egy általam választott perspektívából történő bemutatására vállalkoztam.

Írásomhoz Sandra Grimes és Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed*¹ című könyvét (Egy CIA beszámoló Aldrich Amesről és az által elárultakról, továbbiakban: Könyv), illetve az Amerikai Egyesült Államok Szenátusa Hírszerző Bizottságának jelentését használtam fel². A könyvet író két hölgy a CIA-nál számos beosztást töltött be, jellemzően elemző-értékelőként, többek között az elhárító törzsben. Mindketten Ames kollégái voltak és jelentős szerepet vállaltak kémügyének felderítésében.

Ames rendkívül érdekes történetén keresztül, a forrásanyag által lehetővé tett mértékben szeretném megmutatni az amerikai elhárítás és hírszerzés viszonyának, együttműködésének néhány részletét, azt, hogy hogyan integráltak elhárító tevékenységet egy hírszerző szervezetbe és hogyan gondolkodtak a két titkosszolgálati tevékenység együttműködéséről. Megismerkedhetünk az Ames-ügy

¹ *Circle of Treason: A CIA account of traitor Aldrich Ames and the men he betrayed* - Sandra Grimes and Jeanne Vertefeuille, ISBN 978-1-61251-305-8, 2012 Naval Institute Press

² *An Assessment of the Aldrich H. Ames espionage case and its implications for U.S. Intelligence*, Report prepared by the Staff of the Select Committee on Intelligence United States Senate, U.S. Government Printing Office 84-046 Washington, 1994.

nyomozásának nehézségeivel és következményeivel, amelyek jelentős hatással voltak a CIA belső működésére.

A történetnek magyar vonatkozása is van. Belovai István, volt katonai hírszerző, akit a rendszerváltás előtt beszervezett a CIA, a Fedőneve: Scorpion című könyvében³ azt állította, hogy lebukása Amesnek köszönhető. Az amerikai árulásának egy másik áldozata Vladimir Mikhaylovich Vasilyev ezredes, aki a szovjet/oroszkatonai hírszerzés, a GRU⁴ tisztje volt. Légügyi attaséként szolgált Budapesten és kulcsszerepe volt a magyar katonai hírszerzés által beszervezett amerikai katona, Clyde Lee Conrad⁵ lebuktatásában.

Szeretném hangsúlyozni, hogy publikációmiban nem a történelmileg hiteles eseménysorozatot mutatom be – hiszen csak nyílt források felhasználására volt módom – hanem a felhasznált irodalmat dolgozom fel. A forrásanyagokat a dőlt betűvel jelzett, illetve lábjegyzetként feltüntetett elemző megjegyzéseimmel egészítettem ki.

Ames az ember

Aldrich Hazen Ames (Rick) ízig-vérig amerikai volt. River Fallsban, Wisconsin Államban született értelmiségi családban, Carleton Ceil Ames és Rachel Aldrich Ames legidősebb gyermekeként (két húga volt) 1941. május 26-án. Ames anyja középiskolai angoltanárként dolgozott, apja, Carleton Ceil Ames Burma történelméből doktorált, majd a River Falls State Teacher's College-ban tanított. 1952-ben kereste meg a CIA és vette állományba elhárító elemző beosztásba. A család Washingtonba költözött, majd 1953-ban, amikor Carletont Rangoonba (Burma) vezényelték, oda is vele tartottak. Sajnálatos módon az apa a nyelvtudása mellett nem rendelkezett a jó művelti szakemberhez szükséges kompetenciákkal, így egy negatív értékeléssel és súlyos alkoholfüggőséggel rendelték vissza két év után Washingtonba, és soha többé nem ment tengerentúli szolgálatra. Miután visszatértek Rangoonból, Rick megkezdte a McLean Középiskolát, ahol a dráma és vita szakkörök aktív tagja lett.

Apja biztatására 16 éves korában jelentkezett nyári munkára a CIA-hoz, ahol két nyarat dolgozott logisztikai területen, illetve irodai kisegítőként, az akkori gyakorlatnak megfelelően. Bár ezek a fiatalok már valamennyire ellenőrzöttek voltak a szüleik révén, de a koruk miatt még a poligráfot nem alkalmazták a felvételi eljárásuk során, így viszont nem is férhettek hozzá szenzitív információkhoz.

1959 őszén Ames megkezdte tanulmányait a Chicago Egyetemen. Ez volt az első alkalom, hogy hosszabb időre elhagyta otthonát, de nem volt elég érett, hogy komolyan vegye a tanulást. Mint a középiskolában, itt is aktív tagja volt a dráma tagozatnak, azonban gyenge tanulmányi eredményei és a sok hiányzás miatt végül elbocsátották az egyetemről.

³ BELOVAI István, Fedőneve: Scorpion, Budapest, 1988, ISBN: 9635506724, magánkiadás

⁴ Glavnoye Razvedyvatelnoye Upravleniye – Felderítő Főcsoportfőnökség, katonai hírszerzés

⁵ KOVÁCS Krisztián: Az amerikai katonai elhárítás külföldön végzett művelti tevékenységének sajátosságai a Conrad kémügy tükrében, Szakmai Szemle, Katonai Nemzetbiztonsági Szolgálat, 2015. 1. szám.

Egy helyi színházban kezdett dolgozni, és csak 1962. év elején tért vissza Washingtonba, ahol ismét jelentkezett a CIA-hoz. Júniusra teljes munkaidős irodai dolgozó lett a Műveleti Igazgatóságon, mint dokumentumelemző, gépipró. Március 23-án a belépő poligráf vizsgálaton elismerte, hogy 1961 novemberében barátjával részegen kölcsönvettek egy kerékpárt egy kocsmá előtt és a rendőrök elkapták őket. Ames barátságos, nyitott volt a vizsgálat során, együttműködött, így sikerrel vette az akadályt és a személyi biztonsági ellenőrzése is pozitív eredménnyel zárult. A következő 5 évben a Műveleti Igazgatóságon dolgozott.

Ugyanebben az időben felvették a George Washington Egyetem történelem szakának levelező tagozatára, melyet 1967-ben sikeresen elvégzett.

1962-ben letartóztatták ittas vezetésért, a következő évben gyorshajtásért, majd 1965-ben felelőtlen vezetésért. Jó munkája miatt ugyanakkor előresorolták GS7⁶ fokozatba (kb. főörzszászlós).

Annak érdekében, hogy a műveleti állományba kerüljön, 1968-ban jelentkezett a CIA képzési programjába (Career Training Program – beléptető tanfolyam), amely felvételi eljárás intelligencia tesztből, politikai ismeret felmérésből, személyes interjúból és fizikai felmérésből állt. Ames a szükséges minimumot teljesítette csak, mert sokkal inkább magányos intellektuel volt, nem pedig egy társas személy, aki bármilyen háttérű, kultúrájú személyt be tudna szervezni. A végső értékelés szerint intelligens, természetes, lelkes és szorgalmas, de nem az ajánlott kategória. Azonban a vietnámi háború időszakát élték, és talán más körülmények között nem vették volna fel, de akkor a CIA-nak minden emberre szüksége volt. A tanfolyamon végül megtanulta a titkos kapcsolat szervezésének, tartásának fogásait, így műveleti tiszt lett, illetve megismerkedett az első feleségével, aki szintén a tréningen vett részt. Rick a Műveleti Igazgatóság Szovjet Blokk Osztályára került – ahonnan az apja akkor ment nyugdíjba – GS9 tisztviselői beosztásba (kb. hadnagy rendfokozatnak felel meg).

Milyen volt Ames, mint ember? Sandra Grimes, a Könyv egyik szerzője, először az 1970-es években találkozott vele, karrierjük kezdetén a Szovjet és Kelet-Európai Osztályon. Habár az irodán kívül nem barátkoztak, 1975-re jól megismerték egymást, mivel két másik kollégájukkal együtt autóztak munkába és haza. Ezek az utak jó hangulatúak voltak, baráti hangvételben beszélgettek, magánéleti és műveleti dolgokról egyaránt. Sandy számára Ames az 1980-as évek elejéig kedves fiúnak, jó beszélgetőpartnernek, kellemes társaságnak tűnt. Mint egy szórakozott professzor, allűröktől mentes volt öltözködésében és viselkedésében is. Fésületlen, a zoknija gyakran nem párban volt, az ingét kinötte, és állandóan késett, ha sofőr volt, ha utas. Mindez azonban nem nagyon számított annak idején a munkahelyén. Rick az Rick volt, akinek a társaságát élvezték a munkatársai, de a háta mögött kinevették a külön megjelenése miatt. Ez nem azt jelenti, hogy nemtörődöm ember volt, sőt néha ideges lett, amikor megkérdőjelezték a szakmaiságát. Mindenki egyenlő volt, de ő még egyenlőbb. Sandy szerint ezekben az időkben nyoma sem volt annak, hogy ő lesz a legelvetemültebb áru. Nem volt benne harag, bátorság és lelkileg sem olyan alkat volt.

⁶ GS – General Schedule, az amerikai közalkalmazotti szférában az előmeneteli rend. A CIA-nál is ez van érvényben, ami megfeleltethető a katonai előmeneteli rendnek. Dolgozatomban tisztviselőként hivatkozom az alkalmazotti állományra.

Jeanne Vertefeuille, a Könyv másik szerzője is ebből az időből ismerte, de kapcsolatuk sokkal hivatalosabb volt. Emlékezete szerint Ames enyhén ápolatlan volt, haja borzalmasan állt, a fogai sárgák voltak a dohányzástól, az általa használt szemüvegkeret pedig ódivatú volt. Másik oldalról érdekes beszélgetőtársnak tartotta, tele ötletekkel. Nem az az ember volt, aki untatta volna partnerét a közlekedéssel vagy az ebéd menüvel. Mint annyian mások, akik ismerték őt, úgy gondolta, hogy alkoholfogyasztásának mértéke nem normális. Amesnek alkoholproblémái voltak, szeretett tivornyázni. Reggelente mindig öntött valamennyi vodkát a narancslevébe, nem csak alkalmakkor ivott. Érdekes, hogy sem a feleségei, sem környezete nem tartotta alkoholistának. Fiatalon kezdett inni, amikor problémák voltak a munkájában és két munkahelyi karácsonyi ünnepségen is lerészegedett⁷.

Jeanne szerint van néhány momentum Ames személyiségében és körülményeiben, ami magyarázatot igényel. Először is az apja CIA karrierje relatíve bukás volt, amit Ames is tudott, hiszen olvasta a személyi gyűjtőjét. (Hogy hogyan jutott hozzá, sosem árulta el, de a szabályzók szerint nem lehetett volna hozzáférése). Az anyja viszont egy népszerű tanár volt a McLean középiskolában, apjával ellentétben sikeres volt.

Ames sokak szerint fegyelmetlen volt, és halogatta a dolgait. Sikertelen egyetemi tanulmánya Chicagóban ennek egy korai példája. Bizonyára megfelelő intelligenciával rendelkezett a sikeres végzéshez, de nem tanult és nem járt az órákra. Pályafutása során több főnöke is beszámolt arról, hogy figyelmetlen volt a pénzügyei terén is, illetve volt, hogy a beosztottja értékelését nem készítette el időre, illetve csak utólag, felületes munkát végezve. Ez annyira kirívó volt, hogy az előmeneteli bizottság feljegyzést készített Ames hanyagságáról.

A fegyelmetlensége mellett csak azt csinálta, ami érdekelte, a többi dolgot hagyta elsikkadni. Ha intellektuális kihívást látott, nagyon jó munkát tudott végezni, és azt el is tudta adni, jól érvelt a fontossága mellett. A kábítószerellenes részlegnél végzett munkája során a nemzetközi együttműködésben például nagyon rátermettnék bizonyult. 1969-ben GS10, 1970-ben GS11 besorolásba került⁸.

1969-ben feleségül vette Nancy Jane Segebarthot, aki szintén a CIA-nál, a Hírszerző Igazgatóságon dolgozott elemző beosztásban. Ames az év szeptemberében megkezdte első külszolgálatát Törökországban, Ankarában. Felesége elkísérte, azonban a CIA szabályzói szerint ehhez le kellett szerelnie – bár magasabb beosztásba volt – és soha többet nem is tért vissza a szervezetbe, keserűen véve tudomásul a távozás kényszerét.

A kiküldetés nem volt túl sikeres Amesnek. Az első ankarai évben jó minősítést kaptak, azonban a második és harmadik évben a teljesítménye fokozatosan csökkent, a harmadik év végére pedig már nem tartották alkalmasnak a beosztása

⁷ Ames mértéktelen alkoholfogyasztása élete, karrierje során sok nehéz helyzetbe sodorta, bár ezek mind következmények nélkül maradtak. Nagyon fontos vizsgálni szenvedélyének okát, hiszen visszavezethető a stresszre, ami – mint látni fogjuk – munkahelyi kudarcaiból és ámulásából eredt, vagyis a kémkedés egyik indikátoráról beszélhetünk. Az indikátorok soha nem bűnösséget bizonyítanak, hanem olyan körülményre utalnak, amelyek kísérői lehetnek egy-egy bűncselekmény-típusnak, ezért vizsgálni szükséges az okukat.

⁸ Eddig a fokozatig nem verseny vagy alkalmasság eredménye volt az előrelépés, hanem automatikus volt a rendszer, vagyis a beosztásba töltött éveknek megfelelően rutinszerű volt az előmenetel.

ellátásra. Vezetői ajánlása szerint a hátralévő karrierjét a CIA Központban, Langleyben kellene töltenie. Az Állomásvezetője⁹ jellemzése szerint hiányában volt a szükséges, alapvető képességeknek. Introvertált típus, kapcsolatteremtő képességei hiányoztak. Nem volt sikeres a külföldiekkel, nem tudott hozzájuk viszonyulni, a beszerzésig pedig egyetlen kapcsolatát sem tudta elvinni. Talán ennek volt köszönhető, hogy Ames egy idő után teljes érdektelenséget mutatott a munkája iránt. A végső értékelésében megfeleltet kapott, a minősítője elemző területre javasolta. Ez mélyen érintette, megbántotta Amest. 1988-ban úgy nyilatkozott munkatársainak, hogy az ankarai évek boldogtalanok és sikertelenek voltak, és komolyan fontolgatta, hogy leszerel a CIA-tól.

1972-ben hagyták el Törökországot. Miután hazatértek, Ames a Szovjet Blokk Osztályon kapott beosztást 1973. januárig, amikor orosz nyelvtanfolyamra küldték. Bár a tanfolyamot befejezte, soha nem rendelkezett használható nyelvtudással.

A következő két és fél évben a CIA főhadiszállásán dolgozott az időközben átalakított Szovjet és Kelet-Európai Osztályon. Szakreferensként tevékenykedett pl. az Aleksandr Dmitriyevich Ogorodnik-ügyben. Ogorodnik a szovjet Külügyminisztérium alkalmazottja volt Bogotában, ahol 1974-ben szervezte be a CIA. Később visszatért Moszkvába, ahol továbbra is kapcsolatban maradt az amerikaiakkal. 1977 nyarán a KGB¹⁰ letartóztatta, de öngyilkos lett a kihallgatása előtt egy ciánkapszulával. Bár néhányan vitatják, az az általános nézet, hogy Ogorodnikot a cseh titkosszolgálat ügynöke, Karel Koecher – aki a CIA alkalmazásában állt – buktatta le. Ames élvezte ezt az ügyet, jól is ment neki a munka, és 1974-ben előléptették GS12 fokozatba (őrnagy-alezredes).

1976 augusztusában Amest New Yorkba helyezték. Ez volt a legsikeresebb időszaka, pályája csúcsa, mert nem kellett tippkutatni¹¹, tanulmányozni, beszervezni, hanem „csak” ügynökök foglalkoztatásba vonták be, amelyekben az FBI¹²-jal működött együtt. Azonban az alkoholproblémája ismét visszatért. 1973. december 20-án tartott karácsonyi partin úgy leittasodott, hogy a Belbiztonsági Iroda munkatársainak kellett őt hazavinnie. A következő karácsonykor sem hazudtolta meg önmagát, és egy biztonsági őr félreérthetetlen helyzetben találta egy kolléganőjével. A Belbiztonsági Irodán minden incidensről feljegyzés készült, amelyek a gyűjtőjébe kerültek, de a főnökei nem törődtek vele.

Nagyon jó minősítéseket kapott, bár kiemelték a halogató, részletekkel nem törődő mentalitását is. Jelentéseivel, főleg a találkozó és a pénzügyi jelentései elkészítésével rendszeresen késett. Ennek ellenére több jutalmat és elismerést kapott, és GS13-ba léptették elő, ami majdnem a csúcs volt már.

⁹ Állomás – külföldön működtetett hírszerző szervezeti egység, amely koordinálja, irányítja az adott országban, régióban tevékenykedő műveleti tisztek tevékenységét. A Központ alárendeltségében működik. https://en.wikipedia.org/wiki/Central_Intelligence_Agency (Letöltés ideje: 2017. 07. 31.)

¹⁰ Комитет государственной безопасности – KGB, Állambiztonsági Bizottság, állambiztonsági szolgálat a Szovjetunióban

¹¹ tippkutatás: a hálózatépítés első fázisa, amikor egy meghatározott hálózati funkcióra kiválasztási célból keresünk és számításba veszünk különböző személyeket. <http://osaarchivum.org/files/fa/357/szotar.CEwin.htm> (Letöltés ideje: 2017. 07. 31.)

¹² Federal Bureau of Investigation – Szövetségi Nyomozó Iroda, országos hatáskörrel rendelkező szervezet, amely feladatkörébe tartozik az elhárítás is.

Ügynökei voltak az akkori szovjet ENSZ főtítkár helyettes, Nikolayevich Shevchenko, illetve Sergey Fedorenko. Egy, a Fedorenkoval végrehajtott találkozót követően Ames metróval utazott haza, azonban elhagyta a jegyzetfüzetét, amibe a találkozót jegyzetelte, és amely lebuktatta volna az ügynökét. Azonnal hívta az FBI-t, akik rövid időn belül megkerítették a táskát a füzettel, amit egy lengyel emigráns talált meg. Később, 1980 októberében Ames a szigorúan titkos minősítésű kommunikációs eszközét hagyta őrizetlenül az irodájában, de végül nem kapott fenyítést ezért sem.

A New York-i időszakban Ames házassága egyre rosszabb lett. Több tengerentúli vezénylést is elutasított, mert a felesége a városban akart maradni. A sok visszautasítás negatívan hatott a megítélésére, ezért 1981-ben mégis elfogadott egy mexikói kiküldetést, ahol csoportvezető lett szovjet vonalon. A felesége nem tartott vele, mert nem akarta feladni a jól fizető üzleti munkáját, de úgy gondolták, hogy Mexikó nincs messze, Ames rendszeresen haza tud majd utazni. Ez a döntés egyben a házasságuk végét vetítette előre. Így, mint földrajzilag agglegény, Ames szabad volt. A nagykövetségen kialakult egy olyan baráti társaság, akik szerették a hosszú, alkoholos ebédeket és Ames egyre többet ivott. Senki nem vetette szemére a munka utáni italozást, hiszen egyedül élt¹³.

Egy idő után mentalitása hasonló lett az Ankarában tapasztaltnak. Az amerikai nagykövetségen tartott egyik fogadáson olyan sokat ivott, hogy hangos szóváltásba került egy kubai küldöttel. Máskor közlekedési balesetet okozott, de olyan részeg volt, hogy nem tudott válaszolni a rendőr kérdéseire, és a követség érte küldött tagját sem ismerte fel. A kubaival folytatott vitája miatt az előljárói elbeszélgettek vele, illetve javasolták, hogy az Államokba való visszatérése után vegyék vizsgálat alá az alkoholproblémái miatt.

Visszatérésekor valóban elbeszélgettek vele, de azt nem követte semmilyen kezelés. A vértesztje normális volt, és tagadta, hogy alkoholproblémái lennének. Az egészségügyi szolgálat nem igazán foglalkozott a problémával, sem a Belbiztonsági Iroda, sem a Művelési Igazgatóság.

A mexikói évek alatt az első értékelése jól is sikerült, a második és egyben utolsó elég gyenge volt. Mint Törökországban, itt is megmutatkozott, hogy jobb a hírforrástartásban, mint a szervezésben. A szolgálata során kevés időt töltött az irodán kívül, kevés kapcsolatot létesített és folyamatosan csúszott a pénzügyi jelentésekkel. Az értékelése szerint általában passzív, érdektelen, és a kevéske adminisztratív munkájára fekteti a hangsúlyt, amiben időnként meghaladta az átlagos szintet és jó teljesítményt nyújtott.

A kívülállók számára meglepetésként 1982 májusában GS14 pozícióba léptették elő (alezredes-ezredes) – amit egyesek szerint még a New York-i munkájáért kapott – ami az utolsó előmenetele volt. Szóba került a neve, hogy egy másik latin-amerikai országban állomásvezető-helyettes legyen, azonban a közvetlen vezetője nem támogatta a kinevezést.

A mexikói kiküldetése során a megromlott házassága mellett Amesnek legalább három házasságon kívüli kapcsolata is volt, és elért arra a pontra, hogy már

¹³ Vélhetőleg az alkoholfogyasztás súlyossága összefüggött a munkából adódó stresszel, mivel olyan beosztást töltött be, ahol titkos kapcsolatokat kellett volna szervezni. Mint az a török kiküldetés során kiderült, ez nem ment Amesnek, a kudarc pedig lelkileg megviselhette és az italhoz menekült.

nem akarja megmenteni a házasságát. Ekkor történt a végzetes találkozója Maria del Rosairo Casas Dupuy-jel, aki a kolumbiai nagykövetség kulturális attaséja volt. Rosariot a CIA lakásgazdának és tippkutató-támogató ügynöknek szervezte be. Vagyis jelentett a CIA-nak azokról a személyekről, akikkel találkozott és érdekesek lehetnek az amerikai hírszerzőknek. Mivel a Mexikóba akkreditált diplomata közösség titkáráként is tevékenykedett, így nagyon sok ország képviselőjével érintkezett. A dokumentációk szerint azonban nem hajtott túl sok hasznot a CIA-nak, így csak havi 100 USD javadalmazásban részesült.

Hamarosan kiteljesedett a szerelmük Amessel, habár Rosario sokkal műveltebb volt. Talán úgy gondolta, hogy egy amerikai diplomatával való kapcsolata – akiből még nagykövet is lehet – jól jöhet. Később, mikor kiderült, hogy tévedett – a CIA előmeneteli rendjét megismerte – nagyon csalódott volt. Ames annak ellenére, hogy házas volt, nem nagyon ügykezett diszkréten kezelni a kapcsolatukat, eljártak közös programokra és egyszer még egy a hivatalos partira is magával vitte barátnőjét. Azonban az Ügynökség szabályzatát figyelmen kívül hagyta, mivel hivatalosan nem jelentette külföldi kapcsolatát a vezetőjének, ráadásul egy titkos kapcsolattal létesített szexuális viszonyt.

1983-ban tért vissza az Államokba – használhatatlan spanyol nyelvtudással és egyetlen beszerzés nélkül –, Washingtonba, a Központba került vissza. A Szovjet és Kelet-Európai Osztály szovjet ügyekért felelős alosztályára kerestek embert. Ezek az alosztályok, inkább elemző-értékelő szakemberekre volt szükség – nem is szerették őket a műveltek, akik a területi munkát preferálták – így az üres beosztásokra csak kevés jelentkező volt. A sors kegyének köszönhetően a tengerentúli tapasztalattal, szovjet vonalon dolgozó Ames nagy eséllyel indult, és meg is kapta az alosztályvezetői beosztást, annak ellenére, hogy az állomány körében kisebb felháborodást váltott ki a sikertelen mexikói külszolgálat utáni beosztásba helyezése. A feladata az volt, hogy monitorozza a szovjet ügynökök foglalkoztatását, tárja fel a foglalkoztatásból eredő biztonsági kockázatokat. Ebben a pozícióban Amesnek hozzáférése volt a CIA összes műveletéhez, amelybe szovjet tisztek voltak érintettek világszerte. Belelátott a CIA minden tervébe, amely a KGB és a GRU ellen irányult.

1983 februárjában a Belbiztonsági Iroda rutinellenőrzést hajtott végre Ames vonatkozásában, amely során megállapították, hogy társasági ivó (nem otthon, egyedül iszik, hanem csak társaságban), aki egy kicsit túlbuzgóvá válik, ha több alkoholt fogyaszt. A mexikói előjárója hiába javasolta a konzultációt az osztályvezetőjével, a javaslat nem jutott el a főnökéhez.

1984-től besegített a CIA egyik területi irodájának is a szovjet diplomaták tanulmányozásában. Részvételét annak ellenére hagyták jóvá, hogy elhárító beosztásában hozzáfért a korábbi és a folyamatban lévő műveletekhez. Ames először az FBI-jal koordinálta a kapcsolatát, a részleteket pedig a helyi CIA irodával dolgozta ki. A Szovjet és Kelet-Európai Osztályon Ames jó munkát végzett, a mexikói után sokkal jobb értékeléseket kapott: átlagon felüli szovjet szakértő, jó vezető. Nyoma sem volt az italozó magatartásnak az értékelésében.

Ebben az időszakban, egy szovjet kapcsolattal való találkozót követően Ames folytatta az ivást az FBI-CIA softball mérkőzés alatt, amíg le nem részegedett.

Hazavitték, de a pályánál maradt a jelvénye, rejtjeles dokumentumok, fedőigazolványa és a kabátja. Ennek az esetnek sem lett következménye.

Ames 1984 őszén ismét egy rezsimsértés részese volt, amelybe belevonta Rosariót is. Két kollégájával az Ügynökség egyik „T” házába¹⁴ tervezték beszámoltatni a dezertáló Vitaly Yurchenko KGB ezredest. Ames azonban Rosarioval jelent meg a házban, ami miatt kollégái fel is jelentették, mivel a nő jelenléte dekonspirálta a fedett házat, a műveleti állományt és a tevékenységüket is. Ames a főnökei javaslatára egy hotelba költözött és az ügynök szintén nem volt következménye.

1983 decemberében meghalt Rosario apja, így a nő Ames után ment Virginiába, a Pimmitth Hillsbe bérelt lakásába. Ames felesége még New Yorkban volt, de a házasságuk már véget ért. Rosariónak nem volt munkája, fizetése, hiszen látogatói vízummal tartózkodott az Államokban, ami a munkavállalását korlátozta. Emellett néhány havonta vissza kellett utaznia Kolumbiába, hogy megújítsa beutazási engedélyét. A szabadidejét Ames pénzének költségével töltötte, melyhez alkalmanként az anyja is csatlakozott. Sosem vásárolt az olcsóbb Wall Martban, inkább a Nordstrom és a Nieman Marcus illett hozzá. Nem járt McDonaldsba, inkább éttermekben szeretett enni. Az idő előrehaladtával Ames mind mélyebbre süllyedt az adósságban: feleségének a nyugdíjszámláján, valamint a Virginiában lévő házuk fenntartásának költségein túl válás kiadásait is finanszíroznia kellett. Amesnek 300 USD-t kellett fizetnie 42 hónapon keresztül, 1985 júniusától 1989 novemberéig. Ez 12.6000 USD terhet jelentett számára, továbbá ki kellett fizetnie minden tartozásukat, ami 33.350 USD-t tett ki.

Rick és Rosario 1985 augusztusában házasodott össze, esküvőjük szerény volt. Csak a család és szűk baráti kör volt jelen, köztük Diana Worthen, Ames kolléganője, Rosario barátnője. Rosario ekkorra megszerezte az amerikai állampolgárságot – ami CIA-követelmény volt a házassághoz –, végrehajtották a poligráfos személyi biztonsági ellenőrzését, azonban nem végeztek háttérellenőrzést Kolumbiában. Bár a Belbiztonsági Iroda nem tárt fel semmilyen kockázatot, a Műveleti Igazgatóság elhárító vezetése javasolta, hogy mivel Ames külföldi személyt vesz feleségül, az elhárító alosztály vezetői beosztásából helyezték egy kevésbé szenzitív helyre. A javaslat ellenére sem történt meg Ames áthelyezése.

Ames úgy érezte, hogy csőd fenyegeti. Volt egy autókölcsöne, egy személyi kölcsöne és egyre növekvő hitelkártya tartozása. A lebukása utáni kihallgatása során úgy nyilatkozott, hogy „nagy nyomást éreztem, a pénzügyi helyzetemben. Az előző két évben, amelyet Washingtonban töltöttem, felhalmoztam adósságaimat, új bútorokat vásároltam a lakásba, lakbért fizettem. Összesen kb. 10-13.000 USD tartozásom volt, ami nem túlságosan elkeserítő, de terhelő. Rosario már velem élt abban az időben, családot szerettünk volna, így hosszú távra kellett gondolnom”.

A CIA DO SE Division

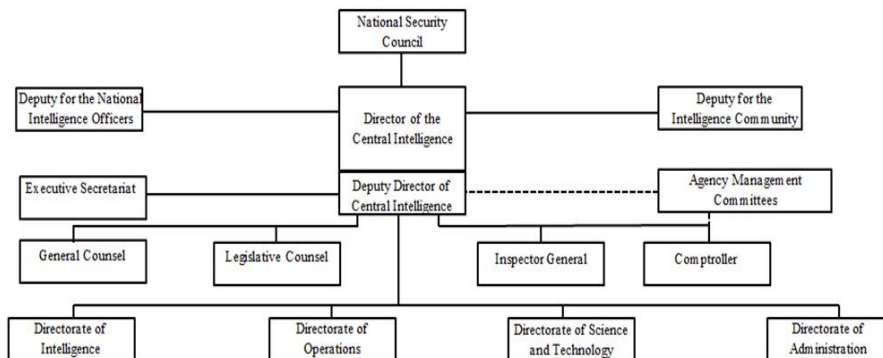
Az Ames kémtörténet számos érdekességének egyike, hogy bár a legjelentősebb amerikai hírszerző szolgálat, a CIA egy munkatársáról van szó, mégsem hírszerző

¹⁴ titkos lakás, amelyet műveleti célra használtak, pl. találkozók lebonyolítása

tisztviselőről, hanem elhárítóról kell beszélünk. Ennek megértéséhez röviden és nagyvonalakban tekintsük át a CIA tevékenységét.

A CIA szervezete számos igazgatóságot foglal magába, az egyik ilyen a műveleti részleg, amelyet 1951-től 1973-ig Directorate of Operations-nek (DO, Műveleti Igazgatóság¹⁵), majd később National Clandestine Service-nek (Nemzeti Titkos Szolgálat) neveztek. A DO feladatkörébe tartoztak a fedett és titkos műveletek, a külföldi ügynökök beszerzése, foglalkoztatása.

Az Igazgatóság többek között politikai, félkatonai, gazdasági és elhárító műveleteket hajtott végre, illetve feladatkörébe tartozott többek között a terrorselhárítás, kábítószerellenes műveletek, HUMINT műveletek, illetve a földrajzi felosztás szerinti hírszerzés.



1. ábra

A Műveleti Igazgatóság helye a CIA szervezetében - 1975-ös állapot

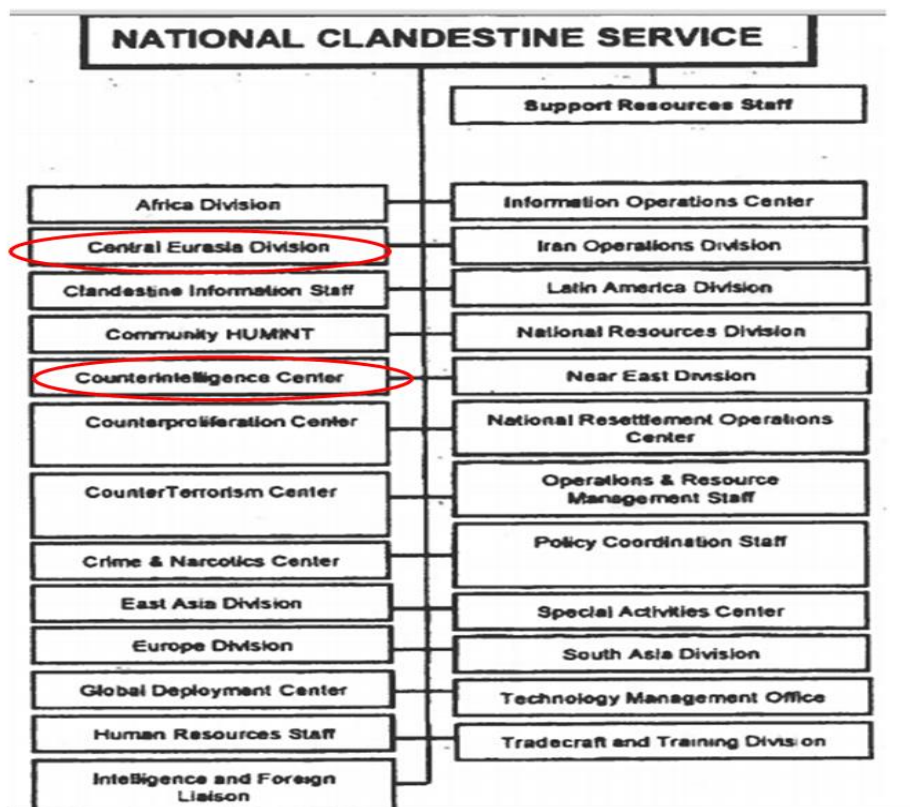
<https://archive.org/details/CIA-Organization-Charts> (Letöltés ideje: 2017. 11. 03.)

A feladatrendszernek megfelelően a DO számos szervezeti egységet foglalt magába, amelyek közül a Counterintelligence Staff-ot (CI Staff, Elhárító Törzs) emelem ki. A Törzs az igazgató alárendeltségében működött, funkciója a támadólagos elhárító műveletek¹⁶ irányítása, vagyis külföldi hírszerző tisztek tanulmányozása, beszerzése és foglalkoztatása, illetve a CIA műveleteket elhárító szempontból történő felügyelete volt, továbbá tájékoztatók, elemzések készítése a többi szervezeti egység számára. A törzs fogta össze az igazgatóság egyes szervezeti egységeibe, osztályaiba integrált elhárító részlegek munkáját.

¹⁵ A szervezeti egység megnevezések félrevezetőek lehetnek a szervezet nagyságának megítélése során, hiszen az Igazgatóság létszáma több ezer főre tehető.

¹⁶ Támadólagos (offenzív) elhárítás: közvetlenül az ellenérdekelt hírszerző szolgálat ellen irányuló elhárító tevékenység, az elhárítás egyik szakterülete. A támadólagosságot lehet értelmezni a kémelhárítás és a terrorselhárítás területén. A célja, hogy az ellenérdekelt hírszerző/terrorista szervezetről, annak működéséről, tagjairól, lehetőségeiről, szándékairól stb. tudjunk meg több információt, amihez be kell épülni a szervezetükbe, ezzel biztosítva a kezdeményezést. A támadólagos elhárítás alapvető eszköze a hálózati személy. Az elhárítás a saját erőket/állományt és a behatolási csatornákat is védi és ellenőrzi a védelmi jellegű (defenzív) tevékenység keretében.

Az alábbi ábrán láthatjuk a Műveleti Igazgatóság – jogutódja – szervezetének egyik verzióját, amelyet 2015-ben tettek közzé.



2. ábra

<https://nsarchive.wordpress.com/2015/10/27/first-complete-look-at-the-cias-national-clandestine-service-org-chart/> (Letöltés ideje: 2017. 07. 31.)

Az ábra már több szervezeti változást követően mutatja be a Műveleti Igazgatóság/Nemzeti Titkos Szolgálat felépítését. Történetünk szempontjából az elhárító részleg a fontos, ami itt már nem Counterintelligence Staff, hanem Counterintelligence Center (Elhárító Központ, 1988-as szervezeti változás nyomán), illetve Ames beosztási helyét, a Central Eurasia Divison-t kell még megemlíteni.

Korábban, 1960 és 1990 között a szovjet és kelet-európai műveletek nagyjából ugyanabban a szervezeti struktúrában működtek. 1966-ban volt egy nagy változás, amikor az East Europe Divison (Kelet-Európai Osztály) egyesült a Soviet Russian Divison-nal (Szovjet-Orosz Osztály), új neve Soviet Bloc Division (Szovjet Blokk Osztály) lett.

Az osztály több alosztályból állt:

- szovjet és kelet-európai elhárító alosztály;
- saját Állomásokat és műveleteket felügyelő alosztály;

- elemző-értékelő alosztály;
- művelettámogató alosztály.

Tehát ennek a műveleti osztálynak is volt egy elhárító részlege, alosztálya, amely felelt azokért a műveletekért, amelyben KGB és/vagy GRU tiszteket szerveztek be, bár tevékenységében az 1970-es évektől működtetett második részleggel volt némi átfedés. Az elhárító alosztály adott elhárító útmutatást, áttekintett ügyeket, tanulmányokat és kutatásokat végzett. Az alosztály volt felelős a Szovjetunió és Kelet-Európa elleni támadólagos elhárító műveletekért, ami a gyakorlatban azt jelentette, hogy a külföldi hírszerző szolgálatok állományát igyekeztek beszervezni. Ez jellemzően a külföldön működő amerikai diplomáciai kirendeltségekkel együttműködő szovjet és kelet-európai személyeket, illetve az Egyesült Államokban működő külföldi diplomáciai testületek tagjait jelentette. Ez a tevékenység, vagyis a külföldi hírszerző szolgálatok tagjainak beszerzése a támadólagos elhárító tevékenység, amely jellemzően az elhárító szolgálatokon belül működik.

A kémelhárítási támadólagos elhárítás csak egy szakterülete (támadólagos) és egy funkciója (kémelhárítás) az elhárításnak¹⁷. A CIA-nál ennél több elhárítási szakterület és funkció (legalábbis a szóban forgó részlegeknél) nem jelent meg, ami determinálta az elhárító tevékenység megítélését. Ez nyomon követhető a CIA-hoz köthető, elsősorban hírszerző területen jártas szerzők publikációiban, amelyek – főleg korábban – jellemzően „csak” a kémelhárításra szűkítették az elhárítást. James McCargar, volt CIA tisztviselő így ír könyvében: „A tudományos érdeklődés egy kisebb eredménye, hogy a történelem szemétdombjára száműzték az általam preferált kémelhárítás – counterespionage – szót és most már elhárításról – counterintelligence – beszélnek¹⁸.

1974-ben a Soviet Bloc Division-t átnevezték Soviet and East Europe Division-ra (SE Division, Szovjet és Kelet Európai Osztály), felismerve hogy Albánia és Jugoszlávia, illetve Románia nem része a blokknak. *Aldrich Ames itt szolgált, az Osztály elhárító alosztályán.*

1988. április 1-jén, egy nagy szervezeti változás keretében létrehozták a Counterintelligence Center-t (Elhárító Központot), *amelynek a tervek szerint – bár az FBI ellenállása miatt ez csak részben valósult meg – illetékességébe tartozott az Egyesült Államok teljes támadólagos elhárító tevékenységének koordinációja, felügyelete.* Feladata a tervezés, a koordináció, valamint az elhárító tevékenység vezetése a CIA-n belül és a Nemzetbiztonsági Közösségben.¹⁹ Az elhárító

¹⁷ Lásd, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényt, amely számos feladatot, funkciót szab a titkosszolgálatok, így az elhárítás számára is.

¹⁸ James MCCARGAR: A short course in the secret war, Madison Books, 2001, első kiadás 1963, ISBN 978-1-5683-3179-9. Itt azt is meg kell jegyezni, hogy a counterintelligence semmiképpen nem hírszerzés-elhárításként fordítandó, hiszen a kémelhárításnál bővebb tevékenységet jelöl. A NATO elvek szerint terrorelhárítást (terrorism), kémelhárítást (espionage), illetve szabotázs (sabotage), felforgatás (subversion), szervezett bűnözés (organised crime) elleni védekezést foglal magába (TESSOC), de a nemzeti feladatkörök országoként eltérően, jellemzően sokkal bővebbek.

¹⁹ Nemzetbiztonsági Közösség/rendszer – Intelligence Community, ami magában foglalja egy ország nemzetbiztonsági szolgálatait, az azokat koordináló, irányító/felügyelő testületeket/személyeket, ellenőrző fórumokat. BÖRCSÖK András ezredes – Dr. VIDA

tevékenység központosítása azt a célt szolgálta volna, hogy összefogja a szétdarabolt CIA elhárító tevékenységet és a CIA-t fókuszponttá tegye a többi elhárítással foglalkozó szervezet között.

Az elképzelések szerint a Központ közvetlenül a CIA főigazgató alárendeltségébe tartozott volna, ami ellen az FBI erősen tiltakozott – még úgy is, hogy felkérték, delegáljon tagot a Központba, de ez sem valósult meg – arra hivatkozva, hogy ez erodálná az ő országon belüli elhárító feladatrendszerüket. Végül a Műveleti Igazgatóság alárendeltségébe került a Központ, ami azért volt különös megoldás, mert azt a látszatot keltette, mintha más igazgatóságoknak nem lett volna elhárítási problémája és máshol nem lett volna szükség az elhárító biztonsági tudatosságra.

A Center három fő területet foglalt magába: Műveleti Csoport, Elemző-értékelő Részleg, Biztonsági Csoport, illetve a támogató egységeket. A Biztonsági Csoportnak két részlege volt: a Nyomozati és a Technikai. Az Ames ügyét, vagyis a kiszivárogtatások ügyét vizsgáló csoport a Nyomozati Osztályhoz tartozott. Ez az osztály volt felelős minden vizsgálatért, ami az Ügynökségbe történő behatolásokkal foglalkozott, ebbe beletartoztak az FBI-től kapott ügyek is. Az osztály vonalas elven dolgozott: pl. szovjet vonal, így itt foglalkoztak az 1985-ös veszteségekkel is. *Nagyon fontos kiemelni, hogy a Biztonsági Csoport nem volt azonos a belbiztonsági szervezeti egységgel!*

1991. december végén a SE Divisonból, Central Eurasian Divison (Közép Eurázsiai Osztály) lett (lásd: 2. ábra).

Érdekes megfigyelni a szervezeti evolúciót. A '60-as években a kelet-európai és a szovjet/oroszműveletek külön szervezeti egységben, majd egy szervezeti egységben, később pedig még nagyobb lépéssel, a közép-európai és ázsiai műveleteket egyesítve jelentek meg. Az összevonásoknak egyik magyarázata lehet, hogy folyamatosan csökkent az intenzitása a nevesített földrajzi térségekből végzett CIA műveleteknek.

Másik fontos momentum, hogy hogyan illesztették be egy hírszerző szervezetbe elhárító elemeket, amelyek jól körülhatárolható szervezeti és feladatkörrel rendelkeztek, ami biztosította, hogy a két feladatrendszer – elhárítás és hírszerzés – elkülönülten tudjon működni. Tehát nem arról volt szó, hogy elhárítók hírszerző tevékenységet végeztek volna, sokkal inkább az volt a cél, hogy a hírszerző tevékenységet megtámogassák elhárító biztosítással, mert úgy gondolták, hogy az elhárító műveleti eljárásrend segíti a saját erőket fenyegető veszélyeket feltárni és elhárítani. A CIA esetében ezért nem beszélhetünk integrált hírszerző-elhárító szolgálatról, mivel az elhárításnak csak egy szűk feladatkörét végezték, végzik, annak érdekében, hogy támogassák fő profiljuk a hírszerzést, vagyis hírszerző szolgálatról van szó. A belső szervezeti elkülönülés is jól mutatja, hogy a CIA esetében is jól el lehet választani az elhárító és hírszerző funkciókat, hiszen ha ugyanazon személyi körnek kellene végeznie mindkét feladatrendszert, az nem tudna megfelelő hatékonysággal működni. A kémelhárítás és a hírszerzés ilyen szoros integrációjának fontosságát Mark M. Lowenthal az alábbiakban foglalja össze:

Csaba mk. alezredes: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására) Nemzetbiztonsági Szemle 2014. II. évfolyam I. szám pp. 65.

„Az elhárítás olyan tevékenységet jelöl, amelynek célja megvédeni saját hírszerző műveleteinket az ellenséges országok és azok hírszerző szolgálatai ellen. Ahogy az 12333 Execution Order (1981; felülvizsgálva 2008) definiálja, a külföldi államok és nem állami szereplők által végzett kémkedés és egyéb tevékenységek elhárítását olyan információgyűjtő és reagáló fázisokra bontja, amelyek során az elhárítás azonosít *[fenyegetést]*, megtéveszt *[ellenfelet, felderítő eszközeit]*, kihasznál/kiaknázt *[ellenfél hibáit, gyengeségeit, műveleti lehetőségeit]*, megzavar *[az ellenfél tevékenységét]*, megvéd *[ellenségtől]*”.

„Az elhárítás egyidejűleg elemző-értékelő és műveleti munka, amely nem egy különálló tevékenység a hírszerzési ciklusban.²⁰ Az elhárításnak át kellene hatnia a hírszerzés minden aspektusát, azonban azt gyakran biztonsági tevékenységként aposztrofálják. De az elhárítás nem pusztán humán információszerzés, nem pusztán fedett művelet, habár részben információgyűjtő tevékenység és fedett műveleti tevékenység is. Nem csak biztonsági tevékenység, mert rendelkezik elemző-értékelő és műveleti képességgel, de egyúttal az is, amikor azonosítja a biztonsági kockázatokat és védelmet nyújt ellenük, azonban mégsem azonos a bűnüldözési tevékenységgel. Összegezve megállapítható, hogy az elhárítás az egyik legbonyolultabb témája a hírszerzésről szóló vitáknak.”²¹

A szovjet/ orosz rendszerben is megfigyelhető hasonló. Ott az elhárításba integrálták a hírszerzést, hiszen korábban a KGB – ami elsősorban elhárító szervezet volt – 1. Igazgatósága volt felelős a külföldi hírszerző tevékenységért. 1991-től a KGB megszűnését követően az elhárítást az FSZB (Федеральная Служба Безопасности – Szövetségi Biztonsági Szolgálat, elhárítás) míg a hírszerzést az SZVR folytatta. Napjainkban pedig, a Putyini reformok eredményeként az SZVR (Служба Внешней Разведки – Külföldi Hírszerző Szolgálat, civil hírszerzés) ismét az elhárítás, az FSZB felügyelete alatt áll.

Kémkedés

1985 tavaszára megérett Amesben a döntés, hogy a pénzügyi helyzetét kémkedéssel próbálja megoldani, ennek érdekében kidolgozott egy tervet, hogy a CIA és az FBI ne szerezzen tudomást szovjet kapcsolatai jellegéről. Munkája révén rendszeres kapcsolatban állt a Szovjet Nagykövetség diplomatáival, amely találkozókra jelentést kellett készítenie és meg kellett küldenie az FBI-nak is. Az ilyen – jóváhagyott – találkozókat használta ki Ames, hogy elérje célját. Az FBI által ügynök-jelöltként tanulmányozott, KGB kötődéssel gyanúsítható Sergey Ivanovich Divilkovskiy sajtókonzullal többször ebédelt együtt. Arra kérte, hogy ha

²⁰ Azt a folyamatot, amely során a felhasználók (politikai döntéshozók, katonai parancsnokok, stb.) feladatot szabnak a titkosszolgálatoknak, amelyek ennek megfelelően információt gyűjtenek, azokat rendszerezik, elemzik-értékelik és kielégítik a felhasználók igényeit, hírszerzési ciklusnak (intelligence process/cycle) nevezzük. Van olyan szemlélet, pl. Mark Lowenthalé, amelyben a folyamat kiegészül a felhasználással és visszajelzéssel is.

²¹ Mark M. LOWENTHAL: Intelligence From Secrets to Policy ISBN: 1483307786 Published 2014. pp. 204.

van olyan személy a követségen, aki szeretne amerikai üzletemberrel találkozni, akkor ajánlja be őt. Divilkovskiy, Sergey Dmitriyevich Chuvakhin nevét adta meg, aki fegyverzetellenőr beosztást töltött be. Ames tájékoztatta is az FBI-t, hogy szeretne nevezettel találkozni, akik mivel Chuvakhin nem kötődött sem a KGB-hez, sem a GRU-hoz, ezért nem tulajdonítottak neki nagyobb figyelmet. A CIA-nak viszont az érdeklődési körébe tartozott, hiszen birtokában lehetett olyan információknak, amelyek fontosak lehetnek az amerikai kormánynak. Ames fedőnevét használva, üzletemberként – ugyanúgy, mint Divilkovskiyjal – vette fel a kapcsolatot Chuvakhinnal 1985 elején.

A szovjet nem nagyon törte magát, hogy megismerkedjen Amessel, de beleegyezett, hogy találkozzanak. 1985. április 16-ára szervezte az első találkozóját Chuvakhinnal, akit meghívott egy italra a Mayflower Hotelbe, ami nem messze volt a szovjet követségtől. Ames meg is jelent, azonban Chuvakhin nem. Néhány vodkamaritínitől megbátorodva, Ames végül átment a követségre, habár tudta, hogy a bejáratnál a portás valószínűleg egy KGB-s, illetve hogy az FBI folyamatosan figyeli a nagykövetség bejáratát.

Ames a diplomata után érdeklődött, akivel sikerült is váltania néhány szót és átadott részére egy, a KGB rezidens valódi nevére szóló borítékot. Elhelyezett ebben egy második borítékot is, amelyet pedig a fedőnévre címzett meg. Természetesen külsős személy nem tudhatta volna a fedőnevet, amit Ames is a CIA/FBI által foglalkoztatott Sergey Motorin vagy Valeriy Martynov beszámoltatásából ismerhetett meg.

A dupla boríték egy üzenetet is tartalmazott. Ames elmondása szerint a moszkvai Állomás két vagy három ügyével kapcsolatos információ volt benne. Azt mondta, hogy úgy hitte, ezek az ügyek a KGB játszmái a CIA ellen, vagyis az átadott információkkal nem árt senkinek. Volt még a borítékban egy kétoldalas telefonszám lista, amely tartalmazta a Szovjet és Kelet-Európai Osztály vezetőinek névsorát, amelyben a saját nevét aláhúzta. Az üzenetben 50.000 USD-t kért az információért, azért ennyit, mert amikor Mexikóban volt, a KGB ennyit ajánlott egy CIA tolmácsnak. Közvetítőnek pedig Chuvakhint javasolta, hiszen vele legálisan tarthat kapcsolatot az FBI és a CIA jóváhagyásával. Mivel Ames nem kereshette volna fel a követséget az FBI előzetes értesítése nélkül – hiszen mindenkit dokumentáltak, aki oda érkezett vagy onnan távozott – később fel is hívta őket, hogy tájékoztatást adjon és bocsánatot kérjen, arra hivatkozva, hogy nagyon dühös volt a lemondott találkozó miatt, ezért cselekedett meggondolatlanul²².

Az előjáték után Ames várt, tudta, hogy a döntéseket nem helyben hozzák, hanem értesítik Moszkvát. Időről-időre felhívta Chuvakhint egy-egy ártatlannak tűnő felvetéssel, miszerint találkozhatnának, tudva, hogy ha még nincs döntés, Chuvakhin elhalasztja a kért találkozót. Május közepén jött az áttérés. Chuvakhin, aki korábban sosem volt kezdeményező a kapcsolattartásban, felhívta Amest és azt ajánlotta, hogy igyanak meg egy italt a szovjet követségen, majd ebédeljenek együtt valahol. Május 15-én Ames megjelent a Szovjet Nagykövetségen, ahol Chuvakhin átadta Viktor Ivanovich Cherkashinnak²³, rangidős KGB tisztnek, Ames első tartójának. Cherkashin, aki tartott az FBI lehallgatásától – feltételezve, hogy az épületük is be van technikázva – vagy attól félve, hogy az egész csapda és Amesnél van valamilyen hangrögzítő, a találkozón nem beszélt, hanem papírra jegyzetelve

²² Ez a fegyelmetlenségnek tűnő magatartás több figyelmet érdemelt volna az FBI, illetve a CIA belső biztonsági részlege részéről, azonban Ames legendája jól működött.

²³ Victor CHERKASHIN – Gregory FEIFER: Spy Handler – Memoir of a KGB Officer, Basic Books, 2005, ISBN 13978046500968

kommunikáltak. Cherkashin tudatta Amessel, hogy a KGB elfogadja az ajánlatot, kifizetik a pénzt, illetve Chuvakhin maradhat összekötő. Az ebéd végül elmaradt, azonban innentől kezdve Ames egy ideig igyekezett tájékoztatni az FBI-t a találkozók megtörténtéről.

Legközelebb május 17-én találkoztak és a közös ebéd alatt a szovjetek kifizették a kért 50.000 USD-t. Innentől kezdve a találkozók rendszeressé váltak és ezekre mindketten vittek egy-egy bevásárló táskát, amit aztán kicseréltek. Ames táskájában minősített iratok voltak, Chuvakhin táskájában pedig a követség sajtótájékoztató anyagai, illetve pénz, vodka, és a KGB üzenetei. Ames minden ebéd után jelentést írt a CIA-nak és az FBI-nak, amiben a találkozó nem operatív vonatkozásait domborította ki. Az volt a célja, hogy úgy mutassa be ezt a kapcsolatot, ami nem haszontalan, ezért nem kell megszakítania, de nem is hoz annyit, hogy bárki fantáziát lásson benne további műveleti lépések tervezésére.

Ames elismerte, hogy motivációja változott az idők során. Először egyalkalmas üzletet akart kötni, a saját kettős ügynökeik átadásával. Azt gondolta, hogy az 50.000 USD megoldja a problémáit. Hogy miért folytatta? Az számára sem volt teljesen világos, a fő ok talán hogy a pénz átvételével döbbsen rá tette abnormalitására. Ami előtte logikus, okos akciónak tűnt, májusra már elveszítette az értelmét. Ames úgy érezte magát, mint egy alvajáró, teljesen összezavarodott, hogy átlépte a határt és hogy annyi pénze volt, amennyit korábban sosem látott. Másfelől saját magát is akarta védeni, ezért árulta el a szovjet tisztek nevét, nehogy lebukassák őt.

Így folytatódott tovább a találkozók júniusban és júliusban, majd Ames jelentései megszűntek. Habár voltak jelek, hogy a találkozók folytatódtak, és az FBI többször is kérte a jelentések aktualizálását, ez nem történt meg. Ames több kifogást is talált a Chuvakhin-ügy pontos dokumentálását elkerülendő. Arra hivatkozott, hogy azért nem volt rá ideje, mert egy másik ügy, illetve annak jelentései elkészítése; a Rosarioval kötendő házasság előkészítése, valamint a leendő olaszországi kiküldetésére történő felkészülés (szeptembertől nyelvtanfolyamra járt és csak péntekenként járt be a munkahelyére) rendkívüli módon lefoglalják. Ez nem lett volna kirívó eset Ames munkájában, hiszen korábban is kellett már figyelmeztetni, hogy időben készítse el a jelentéseit.

A feltételezések szerint Ames június 13-án követte el a „Nagy Kiszivárogtatást”, amivel hatalmas csapást mért a CIA műveletekre. A KGB mindennemű ígérete vagy kérése nélkül találkozott Chuvakhinnal és átadta 10 fő csúcsügynök dokumentációját.²⁴ Ez volt a CIA történelmében az addigi legnagyobb kiszivárogtatás egy találkozón. Kémtevékenysége során egyszerűen nylon zacskóba rakott 2-3 kg táviratot²⁵, dokumentumot és kísértalt vele a főbejáraton, ahol kifelé nem ellenőrizték az alkalmazottakat. A KGB nagyra értékelte ezt a lépést, mivel néhány hónap múlva küldtek Amesnek egy üzenetet: „Gratulálunk, Ön milliomos lett!” Ezzel együtt 2 millió dollárt kapott, illetve felajánlották számára, hogy majd ők őrzik azt. Ezt követően rendszeres fizetséget kapott, 20-50.000 USD-t

²⁴ Ames modus operandija – a mód, ahogy a kémkedést elkövette – szerint az ügynökök gyűjtőit adta át, vagyis azonosította őket, nem pedig áttételes információkat szolgáltatott.

²⁵ Az Állomás és a Központ közötti üzenetváltások

alkalmanként, amelyet számos újonnan nyitott bankszámlára helyezett el 10.000 USD befizetésenként, hogy elkerülje a banki ellenőrzés figyelmét.

Július 31-én Ames és Chuvakhin tervezetten együtt ebédelt Georgetownban. Ames meglepődésére több más szovjet hivatalnok is csatlakozott hozzájuk, köztük Cherkashin is. Az ok, amiért a KGB ezt így szervezte, azt volt, hogy a CIA poligráf vizsgálatát megpróbálják kijátszani. Ha kérdezik Amest, hogy találkozott-e KGB tisztekkel Washingtonban, nyugodtan válaszolhatja, hogy igen. Ames mégis egy nagy dilemmával nézett szembe. Eddig azt jelentette, hogy Chuvakhin nem köthető hírszerző szervezethez, úgy tudta őt bemutatni, hogy az FBI-nak nem volt különösebb érdeke vele foglalkozni. Ha jelenti, hogy Cherkashin is jelen volt, az nagy valószínűséggel felkelti az FBI figyelmét, ami az ügyének nem jött volna túl jól. Ha úgy jelenti, hogy csak ketten voltak, megkockáztatja a lebukást, hiszen az FBI valószínűleg figyelte Cherkashint és a figyelés lebukatta volna Amest is. Ames a megszokott taktikáját követte, a halogatást. Sosem írta meg a jelentést erről a találkozóról, majd a későbbiekről sem, amire mentségül mindig az elfoglaltságát hozta fel. Szóban beszámolt egy-egy találkozóról, amit a területi iroda továbbított az FBI-nak. AZ FBI viszont aggódott, hogy a találkozók mennek és nincs jelentés, ezért kérték a CIA-t, hogy Amessel írassanak jelentéseket. Volt közös egyeztetés is, de további intézkedés nem következett. Évekkel később, miután Ames Rómából visszatért, ismételten kérték, hogy írja meg az elmaradt jelentéseket, de ez soha nem történt meg és nem is volt következménye.

Ames lebukását követő kongresszusi vizsgálat során megállapították, hogy Ames közvetlen főnöke, osztályvezetője engedélyezte számára a kapcsolattartást, de már felügyeleti joga nem volt, hiszen a kapcsolattartás a területi Irodához tartozott. Ők viszont nem tájékoztatták a közvetlen főnökét a jelentések elmaradásáról. Az Osztály rangidős ellenőre, aki beosztásánál fogva rálátott Ames minkét pozíciójára pedig azt nyilatkozta, hogy nem tudott a szovjet hivatalnokkal való találkozókról, mert máskülönben meg is tiltotta volna azt, tekintettel Ames eredeti beosztására.

Ames első négyesemközi találkozója Vladimir Mechulayevvel 1985. decemberében történt Bogotában²⁶, majd a következő években Mechulayev lett a tartótisztje. Ames egy bevásárló központban várt rá, a tartó jelszóval közelítette meg őt. Ezután egy szovjet követségi autóba szálltak és egy szovjet tulajdonban lévő objektumba mentek. A találkozón bemutatkozással kezdtek, sok megbeszélni valójuk volt, többek között a római szolgálat idején követendő kommunikációs terv is. A találkozó elhúzódott és Amesnek ki kellett magyarázni magát Rosario családjá előtt, akiknek a késést a karácsonyi bevásárlással magyarázta. A család, mivel nem jött meg időben Ames, elkezdtek a biztonságáért aggódni, de szerencsére visszatért, még mielőtt a rendőrséget riasztották volna.

Ames főnökei általában úgy ítélték meg, hogy a fejlődéséhez tengerentúli tapasztalatokra van szüksége. Ők ajánlották a római beosztást számára és Ames jelentkezett is, amit 1985. júliusban hagytak jóvá. 1985 októberében megkezdte az olasz nyelvtanfolyamát, de a szovjetekkel a találkozók folytatódtak.

²⁶ A harmadik országos találkozó előnye, hogy a befogadó ország elhárítása elsősorban a saját állampolgárainak ellenőrzésére koncentrál, nem pedig két másik ország képviselőinek találkozására.

Ironikus, hogy az Európai Osztály vezetője, aki jóváhagyta Ames vezénylését, az egyike volt azoknak, aki Ames előjárója volt Ankarában 1972-ben, és akkor még azt javasolta, hogy jobb, ha a Központból nem engedik ki. Mások úgy tartották, hogy Ames kiküldetés egy gyenge láncszem eltüntetését szolgálta a Központból.

1986. május 2-án Amesnek rutin poligráf vizsgálaton kellett részt vennie²⁷. Ames későbbi vallomása szerint, ha tudja, hogy a közeljövőben poligráfozzák nem kezdte volna el a kémkedést²⁸.

Ames visszaemlékezése szerint rendkívül aggódott a poligráf miatt. A kérdések az alábbi témákban voltak: van-e engedély nélküli kapcsolata külföldi hírszerző szolgálattal, engedély nélkül adott-e hozzáférést minősített anyagokhoz, van-e pénzügyi problémája, követett-e el visszaélést. Ames megtévesztő választ adott arra a kérdésre, hogy idegen titkosszolgálat megkérte-e dolgozzon nekik. A vizsgáló megjegyzést tett ehhez a részhez, azonban más kérdéseknél nem volt bizonytalanság. Ames visszaemlékezése szerint azon aggodalmát igyekezett belevinni a vizsgálatba, hogy a szovjetek mindenhol ott vannak, és ez aggasztó kell legyen mindenki számára.

Ezután a vizsgáló tovább kérdezte, annak megértésére érdekében, hogy Ames miért adott megtévesztő válaszokat. Ames közlése szerint, mióta az SE Division-nél dolgozik, volt már bevonva együttműködésbe a potenciális ügynökökkel ezért ismerhetik őt a szovjetek. Továbbá benne van az aggodalom a közelgő római kiküldetés miatt, mert ott is felkérhetik együttműködésre a szovjetek. Ebből a vizsgáló úgy gondolta, hogy Amesben csak az aggodalom nagy, egyébként minden rendben. Úgy értékelt Amest, mint őszinte, nagyon közvetlen személyiség.

Az FBI szerint, akik 1993. júniusban ellenőrizték Ames poligráf eredményeit, az 1986-os eredmények megtévesztés jeleit mutatták, amelyet a vizsgáló nem tárt fel, sőt átsegítette Amest a vizsgán. Annak ellenére, hogy egyértelműen hamis válaszokat mértek, amikor Amest az engedély nélküli minősített anyag hozzáféréséről kérdezték, ezzel kapcsolatban további lépéseket, vizsgálatot, tesztet nem végeztek akkoriban.

A veszteségek

1985 májusában elkezdte a CIA érzékelné a veszteségeket. Júniusban a KGB meghíúsított egy találkozót Moszkvában egy CIA tisztviselő és az elárult szovjet ügynök között. Ekkor még a CIA-tól 1983-ban, drogfogyasztás miatt kirúgott Edward Lee Howardra²⁹ kezdtek fókuszálni, mert egy átállt KGB tiszt, Vitaly Yurchenko ezredes egy bizonyos Robertről beszélt, aki korábban CIA-nál dolgozott és a KGB-nek szivárogtat. Majd szeptemberben és novemberben Moszkvában letartóztattak egy-egy személyt, aztán decemberben egy európai országból visszatérő diplomatát. Mivel Howard ezeket már nem ismerhette, világossá vált, hogy árulása nem magyarázza ezeket az eseményeket. Megszületett az egyetértés, hogy valami rosszul működik.

²⁷ 1976 óta ez volt az első poligráf vizsgálata!

²⁸ Az amerikai gyakorlatban a poligráf alkalmazása általánosan elterjedt az elhárításban (is) és olyan erős indikátornak tartják, ami eldönti pl. egy alkalmazott foglalkoztatását vagy egy ügynök megbízhatóságát. Éppen ezért, valamiféle visszatartó ereje van.

²⁹ Howard később dezertált is a Szovjetunióba. Visszaemlékezéseit a *Safe House The Compelling Memoirs of the Only CIA Spy to Seek Asylum in Russia* című könyvében írta meg, ISBN 978-1882605156

Folyamatosan jöttek a hírek a dekonspirálódott ügynökökről. A CIA észrevétele szerint a KGB meggondolatlanul borította az ügyeket, ami korábban nem volt rájuk jellemző. Ames szerint a KGB-nél is rájöttek a hibára, és elnézést is kértek tőle hogy ilyen helyzetbe hozták, de a politikai vezetőiknek ez volt az elvárása.

Ames több mint 20 ügyet dekonspirált, amihez ha hozzávesszük a Howard és Robert Hanssen³⁰ által elárult személyeket, elmondható, hogy gyakorlatilag összeomlott a CIA szovjet műveleti tevékenysége. 1986. novemberben az SE Division által készített feljegyzés 45 szovjet és kelet európai ügyet tartalmazott, és két technikai műveletet, majd 1987. január 22-én a CIA vezetése úgy nyilatkozott, hogy nagyjából semmijük nem maradt az érdemi információk megszerzéséhez. Kihallgatásán Ames elismerte, hogy az első találkozón 10 ügynököt adott át, összesen pedig kb. 100 ügyről – szovjet és kelet európai – adott információt a tartóinak, de ezekre nem emlékszik pontosan, a nagy szám miatt.

Az amerikaiak egyik technikai művelete GT ABSORB fedőneven folyt, amelynek során a CIA virágcserepbe épített speciális konténereket utaztatott a Transz-Szibériai vasútvonalon. A konténerekben nukleáris aktivitást mérő detektorok voltak, amelyek célja a szovjet titkos atomlétesítmények, nukleáris tevékenység felderítése. 1986. január végén dekonspirálódott a művelet, amikor a szovjet vámosok felnyitották a ládákat.

Minden egyes ügyet a Szovjet és Kelet-Európai Osztály elhárító részlege részletesen megvizsgált annak érdekében, hogy megállapítsák a kompromittálódás okát³¹.

A kérdés az volt, mit tehetnek ellene? Az ügyet szigorúan zártan kívánták kezelni, csak egy szűk kört vontak be a vizsgálatokba. Több verziót állítottak fel arra vonatkozóan, hogy hogyan szivároghattak ki az információk. 1986. januárban egy új szovjet forrás bukkant fel, akit életben akartak tartani, illetve lehetőség adódott arra is, hogy a feltételezéseiket ellenőrizzék. A védelmi intézkedések során abból indultak ki, hogy áruló van az állományukban, vagy a kommunikációs csatornáik dekonspirálódtak. Ebből következően az új ügynököt elektronikai eszközök alkalmazása nélkül kezelték. Egy CIA tisztviselő Washingtonból a Szovjetunióba utazott, több országon keresztül, különböző közlekedési eszköz használatával. Nem jelent meg a nagykövetségen és a munkáját is csak egyetlen CIA tiszt segítette a helyi kirendeltségről, akivel titkos, a diplomáciai kirendeltséghez nem köthető helyeken találkoztak. Ilyen titkos helyen találkoztak az ügynökjelölttel is, illetve a CIA-s tartó jelentéseit a szállodájában írta meg egy kódolt laptopon, visszatért Washingtonba, ahol dekódolták a dokumentumokat³².

³⁰ Robert Hanssen volt FBI tisztviselő, 1979 és 2001 között kémkedett a szovjeteknek/orszoknak.

³¹ A szerzők a könyvükben 30 fő szovjet/országi ügynököt nevesítettek, amiből csak 8 fő volt, akit a CIA vagy FBI szervezett be. A többiek önként jelentkeztek kémtevékenységre, vagy dezertáltak az Egyesült Államokba. A számokból jól látszik a nagyhatalmi pozíció, hiszen az a tény, hogy az amerikaiak egzisztenciát és biztonságot tudtak garantálni – ellentétben esetleg egy sokkal kisebb országgal – jelentősen elősegítette a külföldi hírszerző tisztek meggyőzését ezáltal a saját titkosszolgálat munkáját.

³² Az ügynök foglalkoztatásának lassú és körülményes módja, amit bemutattak, azonban maximális biztonságra törekedtek. Természetesen a laptop kódolt dokumentumokkal való utaztatásának sok veszélye van – hiszen elválasztható a tulajdonosától, és ezzel megszűnik a kontroll feletle – de ettől függetlenül manapság is életképes módszer.

A támadólagos intézkedés abból állt, hogy egy CIA tisztviselő elutazott Nairobi-ba, ahonnan telekommunikációs csatornán hazajelentett egy KGB tiszt sikeres beszerzéséről, bár valójában semmi ilyenről nem volt szó. A tesztnek szánt intézkedés után a szovjetek nem rendeltek haza senkit Kenyából. Ezt lepróbták Moszkvából is, oly módon, hogy küldtek oda táviratot, amelyben a bangkoki KGB tiszt beszerzéséről tettek említést. Ezt követően sem történt válaszlépés a szovjetek részéről, vagyis a kommunikációs csatornák biztonságosak voltak.

1986. januárban drákói intézkedéseket vezettek be, minimalizálták a szovjet ügyekhez való hozzáférést és az Állomások, területi Irodák kommunikációját is csak néhányan láthatták.

1986. január közepén látszólagos áttörés történt. Egy KGB tiszt – aki sosem kapott fedőnevet, csak Mr. X-ként hivatkozták – jelentkezett Bonnban a CIA-nál egy levéllel, azt állítván, hogy a szervezet kommunikációs részlegénél – amely Washingtonon kívül települt – van az áruló. Néhány hónap alatt Mr. X hat levelet küldött, amiből négyben azt erőltette, hogy a kommunikációs részlegen kell keresni a vakondot³³. Természetesen ezek a levelek sok pénzbe kerültek a CIA-nak. Rajta kívül voltak még más önjelöltek is, de ezeket néhány hónap után KGB-s dezinformációs műveletnek nyilvánították az amerikaiak. Ilyen félrevezetési próbálkozás volt korábban pl. Sergey Michajlovich Motorin KGB tiszt esete is, aki 1985. januárig Washingtonban szolgált. Hazatérését követően, áprilisban felhívta a nagykövetségen dolgozó barátnőjét, amiből az amerikaiak arra következtettek, hogy minden rendben van vele, nem bukott le. Később, októberben azonban kiderült, hogy Motorin is hónapok óta letartóztatásban van, vagyis a telefonhívás csak a félrevezetést szolgálta.

Mialatt a CIA próbálta kitalálni mi is történt, Ames 1985. május és 1986. július között 14 alkalommal találkozott a szovjetekkel.

1986 októberéig az SE Divízióknál semmilyen átfogó vizsgálat nem indult. Személyi változásokat követően Jeanne Vertefeuille (a Könyv egyik írója) visszatért Librevilleből (Gabon) a CI törzsbe és kinevezték a Counterintelligence Special Task Force (CI/STF) vezetőjének (elhárító munkacsoport). A munkacsoport négyfős volt, elemző-értékelő szakemberekből állt. Jeanne-n kívül benne volt még Sandy (a Könyv másik szerzője), aki szintén rendelkezett tapasztalattal a szovjet területen, illetve volt még két visszafoglalkoztatott, nyugalmazott specialista is. A csoport összeállításánál nem figyeltek arra, hogy pénzügyi szakértőt vagy nyomozati tapasztalattal rendelkező személyt is beletegyenek. Inkább csak arra figyeltek, hogy olyan embereket keressenek, akiknek van műveleti vagy elhárító tapasztalata, és aki érti a Műveleti Igazgatóság működését. Az is szándékolt volt, hogy a csoport kicsi legyen, mert így a vakond kevésbé szerezhet róla tudomást. A csoport feladata az volt, hogy átnézzék az összes kompromittálódott ügyet és találjanak valami közöset bennük, a motívumot, ami alapján megtalálhatják a kiszivárogtatót.

A munkacsoport által vizsgált kérdések:

- Melyik CIA irodák érintettek az ügyekben?
- Ezekben az irodákban, melyik tisztviselőnek volt hozzáférése az ügyekhez?
- Hány eset köthető Howardhoz? A maradékból hány köthető egyéb okhoz: pl. eljárási hibák?

³³ Vakond: az ellenérdekelte hírszerző szolgálat szervezetbe beépült – beszerzett – ügynöke.

A csoport kereste a mintát, az indikátorokat, de nem készítettek listát a gyanúsítottakról, nem indultak egyének ellen nyomozások, nem vizsgálták azokat az ügyeket, amelyek nem kompromittálódtak – mi lehet ennek az oka – és a vezetőség nem igazán presszionálta őket erre.

Az egység végzett először a CIA történetében számítógéppel támogatott elhárító nyomozást. Először átnézték azokat az ügyeket, amelyek dekonspirálódtak/hattak. Ez óriási munka volt, mert az ügyek minden momentumát percre pontosan dokumentálták, vagyis egy-egy ügy 10-15 vagy még több gyűjtőből állhatott. Másodsorban, mivel nem tudták mit keressenek, minden ügyet aprólékosan, lépésről-lépésre kezdtek el átnézni, megjegyzéseket téve egy-egy fontosnak vélt részletéhez. Jeanne vitte fel ezeket számítógépre, egy 48 mezős táblázatba, amelyben feltüntette az ügynök nevét, a kezdés és befejezés időpontját, helyszíneket, ügyszakmákat, technikai biztosítást adó részleg tagjait, azt, hogy más szervezet ismerte-e az ügyet, más nemzet kapott-e tájékoztatást, volt-e továbbítva valamilyen dokumentum, információ, ami kiszivároghatott és még számos egyéb részletet. A sok részlet dokumentálása ellenére mégis volt, amit kifejejtettek, ilyen volt pl. az ügynök dotálásának valutaneme. Ez fontos adat volt, mert volt, hogy szennyezték a rubel bankjegyet annak követhetősége érdekében. Ebből a megfontolásból pedig újra kellett kezdeni a gyűjtők átnézését.

Ezzel egyidőben a Belbiztonsági Irodán összeírták azon CIA alkalmazottak listáját, akik kiléptek, nyugállományba vonultak, vagy meghaltak 1985-86-ban, azt feltételezve, hogy köztük lehetett a szovjetek embere. Arra gondoltak, hogy a szovjetek azért olyan agresszív módon tartóztatták le az ügynököket, mert a forrásuk már nincs állományban, nem kell aggódni a lebukása miatt. Ezután megvizsgálták, hogy a listán szereplők voltak-e olyan beosztásban, hogy hozzáfértek a bukott ügyekhez. Ennek a vizsgálatnak azonban nem volt használható kimenete.

Az amerikaiak úgy gondolták, hogy a szovjetek 1945 óta az amerikaiakat tekintik legnagyobb ellenségnek, így a KGB a legnagyobb humán erőforrást erre a területre koncentrálna a megfigyelésben, technikai felderítésben, a CIA munkatársainak zaklatásában. A tapasztalatok azonban igazolták a nagy humán erőforrás alkalmazásának sikerét, hiszen a szovjetek nem voltak túl eredményesek – legalábbis a számadatokat tekintve – a CIA munkatársainak megközelítésében. Ez pedig aggodalmat keltett az amerikaiakban, mert azt hitték, hogy a szovjeteknek a fedett műveleteik sikeresek, amelyek nem láthatóak. Ezen feltevés vizsgálatát is megkezdte a Belbiztonsági Iroda, vagyis elkezdte meghallgatni azon CIA személyeket, akik szolgáltak a moszkvai állomáson, vagy hivatalos utat tettek oda 1985-86-ban. Ez a munkafolyamat két évig tartott, de szintén nem hozott eredményt.

Elkezdtek vizsgálni az 1973-tól keletkezett elhárító információkat is, amelyek a CIA-ba történő behatolásokról, vagy ilyen kísérletekről szóltak, de ez sem hozott eredményt.

1986 októberében az FBI megtudta, hogy két forrását kivégezték, így ők is felállítottak egy hat fős csoportot ANLACE Task Force néven, amelynek tagjai teljes munkaidőben a két ügyet vizsgálták.

A CIA és az FBI között nem volt barátságos viszony, de együttműködtek. Az FBI-osok büszkéek voltak, hogy ők műveleti tiszték és nem elemzők, ami persze nem volt teljesen igaz, hiszen nekik is voltak elemzőik, de azokat nem engedték a CIA-val

dolgozni. A két munkacsoport között napi kapcsolat volt, kronológiát készítettek az ügyekről, éjszakába nyúló megbeszélések voltak. Egyik ilyen volt a Farmon³⁴ 1986 decemberében, továbbá a Xerox kiképző központban, Leesburgban, Virginiában, illetve a CIA központban néhány alkalommal. Előfordult, hogy ezeken a megbeszéléseken az NSA³⁵ képviselője is részt vett, a kommunikációs csatorna dekonspirálódásának lehetősége miatt. A teljes együttműködést nehezítette a földrajzi távolság (sic!), hiszen a CIA Langleyben, az FBI Washingtonban székelt, kb. 18 km egymástól. Másfelől, az FBI-nak arra volt mandátuma, hogy saját állományában keressen egy árulót, míg a CIA-nak szélesebb felhatalmazása volt, az, hogy megoldja a problémát.

Az FBI elmondta, hogy számos nyomozati adat az 1970-es évek közepétől arra utal, hogy a CIA-ban áruló van. Az FBI szerint ezek a régi adatok a mostani kiszivárogtatásnak a kulcsai. Ezen felvetés ellen tiltakoztak a CIA munkatársai és feljegyzésükben úgy fogalmaztak, hogy meg kell gondolni, mennyire adják ki magukat az FBI-nak, mennyire működnek együtt. Következésképpen az FBI nem tekinthetett be a CIA vizsgálati anyagába, és nem is kaptak meg minden adatot.

Általánosságban elmondható, hogy 1986-88 között, a két munkacsoport megbeszélésein a CIA adott át releváns részinformációkat, de nem adott hozzáférést a műveleti gyűjtőkhöz/fájlokhoz.

Mindenesetre a második találkozón, 1987 márciusában a CIA elhárító állománya dicsérte a közös munkát és míg korábban sok probléma volt a két szervezet között, az Ames-ügyben kivételes együttműködés alakult ki.

Ennek az együttműködésnek a keretében kidolgoztak egy programot³⁶, amely során 1 millió USD felhasználásával közelítették meg azon KGB tisztet, akiről feltételezték, hogy lehet amerikai ügynökük. A program évekig tartott, az FBI belföldön, a CIA külföldön igyekezett minél szélesebb kör tudomására hozni, hogy 1 millió dollárt adnának, de azt tapasztalták, hogy a KGB legképzettebb és legkevésbé korrumpálható csoportjával állnak szemben.

1986 decemberében kezdődött a Lonetree ügy, amelynek nagy hatása volt nyomozásra. Clayton Lonetree őrmester, aki a Tengerészgyalogos Rendész Zászlóalj³⁷ állományába tartozott, bejelentést tett a CIA bécsi Irodáján, hogy korábban, 1986-ban, amikor a moszkvai amerikai nagykövetségen teljesített szolgálatot, volt egy KGB kapcsolata. Lonetree vallomása szerint, bár tudta, hogy az ilyen jellegű kapcsolattartás szabályellenes, beleszeretett egy orosz nőbe, Violeta Seinába, aki szintén az amerikai nagykövetségen dolgozott. Violetta bemutatta nagybátyjának, Sashának, aki valójában egy KGB tiszt volt. Valódi neve Aleksey Yegorov, aki Aleksey Iefimov fedőnéven dolgozott. A kezdetben barátságos nagybácsi elkezdett érdeklődni a nagykövetség személyzete felől, Lonetree pedig

³⁴ A Farm – Virginia államban, Williamsburg közelében található a Camp Peary katonai bázis és gyakorlótér, amely helyt ad a CIA, DIA és egyéb titkosszolgálat műveleti kiképzéseinek. Ezt a helyet hívják a köznyelvben Farmnak.

³⁵ National Security Agency – Nemzetbiztonsági Ügynökség, a Védelmi Minisztérium alárendeltségében működő titkosszolgálat, amely többek között rádiófelderítéssel, kódfejtéssel, kritikus informatikai infrastruktúrák védelmével foglalkozik. Tevékenysége során kiszolgálja az elhárító és hírszerző szolgálatokat, illetve a katonai műveleteket is.

³⁶ Az FBI-nál Bucklure – Dollárscapda, a CIA Racketter – Zsaroló fedőnevet kapta

³⁷ Marine Corps Security Guard – a tengerészgyalogság diplomáciai testületek őrzését végző egysége

amire tudott válaszolt. Később Lonetreet Bécsbe helyezték és a Sasha be akarta mutatni egy ottani barátjának, Yuriy Lysovna, aki szintén a KGB tisztje volt. Lonetree ekkor eszmélt rá, hogy mi történik körülötte. A nyomozást a Tengerészeti Nyomozó Szolgálat (Naval Criminal Investigative Service) végezte, akik nagyon sok tengerészt meghallgattak, azonban ők inkább bűnügyi nyomozó szakemberek voltak, nem kémelhárítók, így nem tudtak semmit a moszkvai állomásról, a KGB módszereiről, behatolási tevékenységéről. Ennek következtében a meghallgatások során fontos kérdések nem lettek feltéve, megválaszolva.

A CIA csoport a Lonetree ügy felé fordult, és úgy érezték, a moszkvai állomás lehet a kulcs a '85-ös veszteségek megoldásához. A korábban létrehozott számítógépes adatbázisban volt egy olyan mező, ami azt tartalmazta, hogy a moszkvai állomáson ismertek-e minden olyan ügyet, amely dekonspirálódott. A Lonetree ügy miatt alaposabb vizsgálatnak vetették alá ezt a szempontot. Újra elővették a dossziékat és végignézték őket, hogy Moszkva mikor és hogyan tudott ezekről az ügyekről³⁸.

1987. március közepén új intenzitással folytatódott a vizsgálat. Lonetree egyik kollégája, Arnold Bracy tengerész úgy nyilatkozott, hogy ismeretei szerint nevezett egyszer beengedett szovjeteket – a KGB-t – a követségre, a CIA részlegébe és kommunikációs helyiségébe.

Ennek az információnak drámai hatása volt a CIA Special Task Force-ra. Azt feltételezték, hogy ha bejutottak a követségre, hozzáférhettek a műveleti anyagokhoz is. Hónapokat töltöttek el azzal, hogy kitalálják, ebben az ügyben mihez volt/lehetett hozzáférése a KGB-nek. Jött a kérdés, ha a KGB be tudott épülni a követségre, mit érthettek el vele? A vizsgálók beszerezték az őrség beosztását, ami óriási mennyiségű papírt jelentett. Meghallgatták az állomás CIA állományát, hogy mikor van lehetőség a beépülésre, hogyan lehetne nyitni a zárat, riasztót, mennyi idő kell a dokumentumok lefényképezéséhez stb.

A vizsgálat hónapokig tartott, de nem hozott igazi eredményt. Találtak néhány alkalmat, amikor a KGB bejuthatott, de ezek nem voltak meggyőzőek, nem lehetett megállapítani, hogy a KGB valóban be is épült. A vizsgálódás során átnézték minden táviratot, amit a moszkvai állomással forgalmaztak, és kiértékeltek mindenkit, aki, vagy akinek a kapcsolata kompromittálódhatott. Az új projekt Moszkva Munkacsoport néven futott, amelyet maximum 6 hónapra terveztek, időközben belevonták a leningrádi (Szentpétervár) Állomást is. Azonban amint előkerültek az iratok, megdöbbenve detektálták annak hatalmas mennyiségét, a mintegy 60.000 oldalt. Az elkészült jelentés számait, következtetéseit és ajánlásait azonban a Műveleti Igazgatóság vitatta és nem is fogadta el.

Ráadásul, Bracey visszavonta az állítását, Lonetree pedig tagadta, amit a poligráf meg is erősített. 1987. augusztusra odáig jutottak, hogy az egész ügy nem releváns a vizsgálat szempontjából. Eközben persze az eljárók részéről erős volt a nyomás, mert minél hamarabb tudni szerették volna az esetleges kár mértékét.

1987 augusztusában Lonetreet a bíróság 30 évre ítélte, de végül 1996-ban szabadulhatott. A bírósági eljárást követően Lonetree még sok meghallgatáson ment keresztül, amit kombináltak poligráfós vizsgálatokkal, videofelvételes testbeszéd-

³⁸ Lonetree esete tipikus honey trap – méz csapda – amikor egy nő szexuális szolgáltatását és/vagy rajta keresztül érzelmi zsarolást használnak fel információszerzésre a titkosszolgálatok. A férfi megfelelőjére a Rómeó spy – Rómeó kém – elnevezést alkalmazzák.

elemzéssel. Ezekből a vizsgálatokból arra következtettek, hogy Lonetree sosem engedte be a KGB-t a követségre. Ez pedig azt jelentette, hogy majdnem egy évet eltöltött a vizsgálócsoport feleslegesen ezzel az üggyel.

A nyomozás széttöredezett. Elveszítette a prioritást, mert a Szovjet és Kelet-Európai Osztály egyébként sikeresen tevékenykedett. Az 1985-ös veszteségekre olyan történelmi hibaként tekintettek, amelyek már szinte nem is léteztek. Tovább homályosította a helyzetet azon vélekedés, hogy minden kompromittálódott ügy 1985 előttre nyúlt vissza. Pl. Polyakov tábornok már évek óta nyugállományban volt, amikor 1986. júliusban letartóztatták. Másik nagy veszteség volt Vladimir Mikhaylovich Vasilyev, GRU tiszt, aki Budapesten szolgált. De ilyen személy volt Vladimir Viktorovich Potashov, aki 1981-ben jelentkezett, mint az Amerikai Egyesült Államok és a Kanada Intézet kutatója. Őt az FBI és a CIA közösen foglalkoztatatta, majd visszatért a Szovjetunióba és csak később, 1986 júliusában tartóztatták le. Egy másik KGB tiszt, Boris Nikolayevich Yuzin, akit az FBI szervezett be. Nem volt már vele kapcsolat 1982 óta, de csak 1986 decemberében tartóztatták le. Ezen személyekről nem csak Ames tudott, hanem más árulóvá vált titkosszolgák is, mint pl. Richard Hanssen, Edward Lee Howard vagy Earl Edwin Pitts, vagyis nem tudták a lebukásukat egyetlen személyhez kötni. Az elhárító törzsben ezért nem mindenkinek volt a fő hangsúly a '85-86-os veszteségeken, azon csak a szűk csoport dolgozott. A csoport viszont rákényszerült, hogy más árulásokkal is foglalkozzon, ezek pedig elvették az időt a fő feladatuktól.

1985. október elejétől fogva a következő néhány évben KGB törekedett meggyőzni az FBI-t és CIA-t, hogy az Ames által elárult források vagy még mindig életben vannak, vagy nem a CIA-ba beépülés miatt buktak le.

Ilyen akciók voltak:

- a KGB azt híresztelte mindenütt a szervezetén belül, hogy Howard volt az áruló;
- az általuk ismert CIA kapcsolatoknak dezinformációt adtak, miért voltak a többiek letartóztatva, majd őket is letartóztatták;
- a KGB igyekezett a letartóztatott ügynökök körülményeiről azt elhitetni, hogy jól vannak, élnek, pl. a letartóztatott tisztjüket kényszerítették, hogy felvegye a kapcsolatot egy, az Egyesült Államokban élő személlyel, azt közvetítve, hogy szabad és jól van;
- szovjet hivatalos személyek, akik kapcsolatban voltak a CIA-val, olyan információkat igyekeztek csepegtetni, miszerint a lebukások a rossz eljárások miatt vagy személyi hibák miatt történtek.

A CIA és FBI nyomozócsoportnak minden próbálkozást egyenként kellett megvizsgálni. Néhány azonnal kétséges volt, mások hihetőbbnek tündek és további vizsgálatot igényeltek, és akadtak teljesen homályos ügyek is. A CIA-nál érezték, hogy valami folyamatban van, de konkrétan nem tudták megfogalmazni a problémát és csak jóval később ismerték fel, hogy a KGB elterelő eljárásának részei voltak.

Vasilyev³⁹ és Belovai

Az Ames ügynek több szálon is volt magyar vonatkozása, amelyek a Clyde Lee Conrad történettel⁴⁰ voltak összefüggésben. Clyde Lee Conrad főtörzsőrmester, az Amerikai Egyesült Államok hadseregének tagja, 1978 és 1988 között folytatott kémtevékenységet a magyar katonai hírszerzés és áttételesen a Szovjetunió számára. Conradot az amerikai elhárítók a CIA ügynökeinek segítségével tudták azonosítani, aki(k) jelezték, hogy az Európában állomásozó amerikai haderőtől számtalan minősített hadműveleti dokumentum érkezik Moszkvába.

A CIA egyik orosz ügynöke, Vladimir Mikhaylovich Vasilyev ezredes volt, aki a szovjet katonai hírszerzés (GRU) tisztjeként, légügyi attasé beosztást töltött be Budapesten. A magyar hírszerzők által megszerzett dokumentumok rajta keresztül jutottak el Moszkvába, így betekintése volt azokba. Vasilyev ezredes 1982-ben jelentkezett önként az Amerikai Egyesült Államok budapesti nagykövetség katonai képviselőjénél – valószínűsíthetően a katonai attasénál – aki átadta őt a CIA-nak. A fedőneve GTACCORD lett.

Az átadásnak nem igazán örült Vasilyev, aki nem bízott a CIA-ban, ő sokkal inkább katonákkal szeretett volna együttműködni, akiket a munkájából kifolyólag már ismert. Ráadásul a tartója egy nő lett, ami még jobban frusztrálta az orosz ezredest. Végül is hathatós katonai segítséggel sikerült kialakítani egy eléggé korlátozott, de rendkívül produktív együttműködést. Nehéz volt a kommunikáció megszervezése, ami miatt a kapcsolattartás elég rendszertelen volt. További problémát okozott, hogy az amerikaiak nem értették az attasé motivációját és hozzáférését az információkhoz. Az átadott anyagok a Németországi Szövetségi Köztársaságban állomásozó amerikai haderő szigorúan titkos hadműveleti dokumentumait tartalmazták. A CIA kelet-európai forrásai révén már 1978-ban figyelmes lett a kiszivárogtatásra, amiről már akkor tájékoztatták az FBI-t és az FCA⁴¹-t, azonban 1982-ig ezek az információk anekdota-jellegűek voltak, így a nyomozás évekig nem jutott előrébb.

Vasilyev segítségével már konkrét dokumentumok voltak a kezükben, azonban a szovjet attasé sem tudta azonosítani a forrást. Azt elmondta az ezredes, hogy a magyar titkosszolgálat azonnal továbbítja a dokumentumokat a GRU-nak, ami állja a megszerzés költségeit. Végül a Vasilyev féle dokumentumok jelentették a megoldást Clyde Lee Conrad és társai kémtevékenységének felszámolásához. Eközben viszont az ezredes is dekonspirálódott. Először Edward Lee Howard árulta el 1984 végén, az első találkozóján a KGB-vel. Howard, bár nem tudta a szovjet tisztet azonosítani, Bécsben jelentett egy ismeretlen KGB-s ezredesről, akit a CIA Budapesten szervezett be. A szovjet kém Howard mérges, elégedetlen személyként jellemezte, ami arra vonatkozhatott, ahogy Vasilyev érzett a CIA bánásmódja miatt. Howard úgy tudta, hogy a KGB tisztjéről van szó, és mivel a nevét sem tudta, így a szovjetek a Magyarországon szolgáló KGB ezredesekre – akiből több volt – nyitottak nyomozást, a GRU tisztjeire nem figyeltek. Ennek

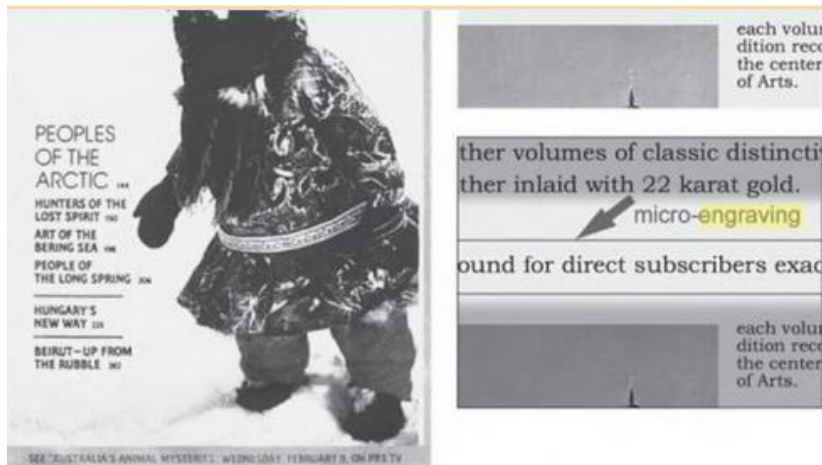
³⁹ <http://fanread.ru/book/10716632/?page=39>

⁴⁰ KOVÁCS Krisztián: Az amerikai katonai elhárítás külföldön végzett műveleti tevékenységének sajátosságai a Conrad kémügy tükrében, Szakmai Szemle, Katonai Nemzetbiztonsági Szolgálat, 2015/1. pp. 35-64.

⁴¹ Foreign Counterintelligence Activity – Külföldi Elhárító Részleg, az amerikai haderő egyik elhárító szervezete volt, amely a külföldön állomásozó csapatok elhárító biztosításáért felelt. Ők nyomoztak Conrad után, akit 1986. januárban sikerült azonosítani, majd 1988-ban tartóztattak le.

eredményeként a nyomozás eredménytelenül elhalt, Vasilyev pedig külszolgálata lejártával új beosztást kapott Moszkvában, ahova 1984-ben tért vissza. Hazatérését követően a CIA-tól kapott egy részletes útmutatást – *kommunikációs terv* – arra vonatkozóan, hogyan tudnak kapcsolatban maradni a Szovjetunióban is, és sikeresen meg is kezdődött az együttműködésük Moszkvában.

Érdekesség, hogy a CIA a '80-as években kifejlesztett lézer-gravírozást használta üzenetküldésre, amely során az ügynök által hozzáférhető újság – ebben az esetben a National Geographic – egyik fekete nyomtatású részében mikroszkopikus üzenetet tudtak elrejteni. Ez szabad szemmel nem volt látható, csak 30-szoros nagyítással. Ezzel a módszerrel közölték a kommunikációs tervet Vasilyevvel, akivel évekig sikeresen tartották a kapcsolatot.⁴²



3. ábra

A nyíllal jelölt fekete keretbe rejtették el a titkos üzenetet.

1985 augusztusában már látszottak a bajok a CIA szovjet kapcsolati körül, ezért szóba került a további együttműködés felfüggesztésének lehetősége. Ezt az ötletet végül is elvetették és tovább folytatták az információcserét GTACCORD-dal, aki utoljára 1985. december 11-én töltött postaládát.

És végül nem volt szerencséje Vasilyevnek, mert Ames árulása már megpecsételte a sorsát. Mivel a CIA Műveleti Igazgatóság Szovjet és Kelet-Európai Osztálya foglalkoztatta, így Amesnek közvetlen hozzáférése volt még a táviratokhoz is. Valószínűsíthetően 1985. június 13-án – a „Nagy Kiszivárogtatás” során – tájékoztatta a szovjeteket a budapesti attaséről, akit azonban csak 1986 júniusa után tartóztattak le. Eközben eltelt egy év. A letartóztatás késedelmének oka lehetett, hogy Howard, Ames és Hanssen árulásának köszönhetően a KGB kapacitását meghaladó számú nyomozást kellett elvégezniük. Volt egy prioritási listájuk, ami szerint először a külföldön lévő KGB és GRU tiszteteket buktatták le, akik nem voltak

⁴² Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda, Robert WALLACE, H. Keith MELTON, Henry R. SCHLESINGER, ISBN 978-0-525-94980-0, 2009. p. 433.

erős kontroll alatt. Őrizetbe vételükhöz először hazacsalták őket, amihez változatos legendát találtak ki, ugyanis ha tömeges letartóztatásba kezdtek volna Moszkvában, a külföldön lévők azonnal dezertálnak. Amikor a művelet első szakasza lezárult kb. 1985. november közepén, kezdődhetett a második szakasz, az odahaza tartózkodók elfogása.

Visszatérve az 1985. decemberi postaládatöltéshez, ez volt az utolsó kontakt. Az Ames Kárfelmérési Csoport, ami 1994-ben, Ames letartóztatását követően kezdte meg működését azt valószínűsítette, hogy az utolsó csomag már a KGB által kreált dokumentáció volt, hogy félrevezessék a CIA-t, elhíthessék velük, hogy Vasilyev jól van és továbbra is együttműködik. Habár a csomag értékes információkat tartalmazott sok témában, nem volt elhárítási relevanciája.

Vladimir Mikhaylovich Vasilyev ezredest hazaárulásért kivégezték.

A másik magyar szál Belovai Istvánhoz kötődik, aki az MNVK 2. Csoportfőnökség (a magyar katonai hírszerzés) tisztje volt alezredesi rendfokozatban. Beosztásából adódóan 1978-tól betekintési jogkörrel rendelkezett a Conrad által átadott minősített amerikai dokumentumokba. 1982-ben Londonba vezényelték, katonai attasé-helyettesi beosztásba, ahol a CIA 1984-ben beszervezte, de még ugyanebben az évben hazarendelték. A magyar hatóságok 1985. július 10-én tartóztatták le, amikor magához vette a CIA által elhelyezett un. konténert, ami az ügynök és tartótisztje közötti konspiratív kommunikációt, anyagok cseréjét, továbbítását szolgálta. A bíróság Belovait életfogytig tartó fegyházbüntetésre ítélte. 1990-ben szabadult elnöki kegyelemmel. Ezt követően elhagyta Magyarországot és az Egyesült Államokban telepedett le, ahol 1992-ben állampolgárságot kapott és katonai nyugdíjat folyósítottak részére. 2009. november 6-án hunyt el Denverben. A feldolgozott irodalom szerint Ames 1985. április 16-án lépett kapcsolatba a szovjetekkel és a „Nagy Kiszivárogtatás” június 13-án vagy 17-én történt. Belovait július 10-én tartóztatták le, vagyis ha csak az időpontokat nézzük, lehetséges, hogy Ames árulta el. Azonban Ames modus operandija szerint, az ügynököket azonosította, aktáikat átadta a szovjeteknek, míg Belovait a magyar elhárítás a letartóztatásakor nem ismerte. Tetteiről az elhárítók a dekonspirálódott postaládát őrizték – valószínűleg a töltő amerikai hírszerzőt követhették – és várták, ki fogja azt üríteni. Vagyis a minta eltér, tehát gyengíti – de nem zárja ki – Ames bűnösségének teóriáját. Másfelől, erősíti – bár nem bizonyítja – az árulás verzióját az a körülmény, hogy a Könyvben kelet-európai ügynökök lebuktatásával is vádolták Amest, bár konkrétumot nem említenek.

Az előzőekben feltárt események azonban még korántsem jelentik történetünk végét. A második részben megismerhetjük azt az időszakot, amikor Amest Olaszországba vezényelték külszolgálatra és hogy ott hogyan alakult a kémtevékenysége. Nyomon követhetjük, hogy hazatérését követően hogyan alakult a CIA vizsgálata és vajon az FBI nyomozhat-e egy CIA tisztviselő vonatkozásában. Végül pedig láthatjuk, hogy a felügyeleti szerv – a civil kontroll – hogyan korrigálja egy nem megfelelően működő titkosszolgálat eljárásrendjét.

Felhasznált irodalom:

- An Assessment of the Aldrich H. Ames espionage case and its implications for U.S. Intelligence, Report prepared by the Staff of the Select Committee on Intelligence United States Senate, U.S. Government Printing Office 84-046 Washington, 1994.
- BELOVAI István: Fedőneve: Scorpion, Budapest, 1988, ISBN: 9635506724, magánkiadás
- BÖRCsök András ezredes – Dr. VIDA Csaba mk. alezredes: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására) Nemzetbiztonsági Szemle 2014. II. évfolyam I. szám.
- CHERKASHIN, Victor– Gregory FEIFER: Spy Handler – Memoir of a KGB Officer, Basic Books, 2005, ISBN 13978046500968
- Circle of Treason: A CIA account of traitor Aldrich Ames and the men he betrayed - Sandra Grimes and Jeanne Vertefeuille, ISBN 978-1-61251-305-8, 2012 Naval Institute Press
- KOVÁCS Krisztián: Az amerikai katonai elhárítás külföldön végzett műveleti tevékenységének sajátosságai a Conrad kémügy tükrében, Szakmai Szemle, Katonai Nemzetbiztonsági Szolgálat, 2015. 1. szám.
- LOWENTHAL, Mark M.: Intelligence From Secrets to Policy ISBN: 1483307786 Published 2014.
- MCCARGAR, James: A short course in the secret war, Madison Books, 2001, első kiadás 1963, ISBN 978-1-5683-3179-9.
- Spycraft: The Secret History of the CIA's Spys, from Communism to Al-Qaeda, Robert Wallace, H. Keith Melton, Henry R. Schlesinger, ISBN 978-0-525-94980-0, 2009.
- <http://osaarchivum.org/>
- <https://nsarchive.wordpress.com>
- <https://archive.org/>

DR. GYARAKI RÉKA

JOGI SZABÁLYOZÁS A NEMZETI ELEKTRONIKUS ADATVAGYON, AZ AZT KEZELŐ INFORMÁCIÓS RENDSZEREK, LÉTFONTOSSÁGÚ INFORMÁCIÓS RENDSZEREK ÉS RENDSZERELEMEK BIZTONSÁGÁRÓL

1. Bevezetés – a jogi szabályozottság

A nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, az azt kezelő információs rendszerek, létfontosságú információs rendszerek és rendszerelemek biztonsága feltétlen nemzeti érdek az információs társadalmat érő fenyegetések miatt. A hazai jogi szabályozás a kibertér védelmével kapcsolatos társadalmi elvárásoknak tesz eleget, amikor az állam és az állampolgár számára biztosítja az elektronikus információs rendszerben kezelt adatok hármaskövetelményét (bizalmasság, sérthetlenség és rendelkezésre állás), valamint rendszerelemei sérthetlenségének és rendelkezésre állásának zárt, teljes körű, folyamatos és kockázatokkal arányos védelmét.

Az elektronikus információbiztonság 2013. július 1-jén hatályba lépett törvényi szabályozása, majd módosításai és a törvényi felhatalmazás alapján kiadott több kormányrendelet igazolják, hogy a kibertérből jelentkező fenyegetések tartalmukban és veszélyességük tekintetében változnak, így a védelemben és a biztonság megteremtésében a létező kockázatok kezelésére alkalmazott eszközök mellett újabb stratégiák kidolgozása szükséges.

A téma leginkább az alábbi jogi szabályzókon keresztül ismertethető: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.), továbbá annak végrehajtási rendeletei, így

- a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolására vonatkozó követelmények,
- a 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat-és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról,
- a 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.

A fent nevesített jogszabály és végrehajtási rendeletei mellett kiemelten foglalkozom a Magyarország Nemzeti Kiberbiztonsági Stratégiájával, azaz a

1139/2013. (III. 21.) Korm. határozattal, a nemzeti adatvagyon szabályozását tartalmazó a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló törvénnyel és annak végrehajtási rendeletével¹.

Nem kisebb figyelmet érdemelt a tanulmány megírása során – a teljesség igénye nélkül – természetesen Magyarország Alaptörvénye, a honvédelemről, a nemzetbiztonságról szóló törvények, valamint a létfontosságú rendszerek és létesítmények azonosításáról szóló 2012. évi CLXVI. törvény (továbbiakban: Lrtv.) és annak végrehajtási rendelete is.

1.2. Intézményi és fogalmi meghatározások

Az Ibtv. meghatározza mind a magyar kibertér, mind pedig a globális kibertér fogalmát. A tanulmány címének megfelelően fontosnak tartom a magyar kibertér meghatározását idézni: *„a globális kibertérellektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne.”*

A nemzeti adatvagyon fogalmát a 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartásokról szóló jogi szabályozás a következőképpen határozza meg: a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége². A fogalomban meghatározott „közfeladatot ellátó szervek” meghatározás alatt értendők az állami és önkormányzati szervezetek, az állami szervek által alapított gazdasági társaságok valamint az állami tulajdonban lévő gazdasági társaságok. A nemzeti adatvagyonnal, mint védendő „tárggyal” kapcsolatos szervezetek feladatait többek között az Ibtv. határozza meg, továbbá magára a nemzeti adatvagyonra vonatkozó jogszabály is tartalmazza.

A címben szereplő másik fogalom a létfontosságú információs rendszerek, amely alatt az általános szóhasználatban a kritikus információs infrastruktúra kifejezést szokták alkalmazni és amit a Zöld Könyv³ határoz meg: *„A kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.)”*

A nemzeti adatvagyon védelme, bár mindenki feladata a szenzitivitása miatt, ennek ellenére nem valamennyi szervezet ezzel kapcsolatos feladatát kívánom ismertetni, hanem kifejezetten a Magyar Honvédség, a Katonai Nemzetbiztonsági

¹ 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló vhr.

² 2010. évi CLVII. törvény 1.§ (1) bekezdése alapján

³ Zöld Könyv A létfontosságú infrastruktúrák védelmére vonatkozó európai programról, COM(2005) 576 final, Európai Bizottság Brüsszel, 2005. 11. 17.) <http://ec.europa.eu/transparency/regdoc/rep/1/2005/HU/1-2005-576-HU-F1-1.Pdf> (Letöltés ideje: 2017. 10. 27.)

Szolgálat és a Nemzeti Kibervédelmi Intézet tevékenységeit, jogköreit vizsgálom meg.

2. A magyar kiberbiztonság szabályozása

A kiberbiztonság szabályozásának szükségessége a kibertérből érkező és megszorodó fenyegetések, támadások miatt elengedhetlenné vált. Ezen fenyegetések kezelése, a támadások elhárítása nemcsak az állami szervezetek, hanem a magánszektor egyes szereplőinek a feladata is.

Magyarország Nemzeti Kiberbiztonsági Stratégiája az „első” jelentős jogi szabályozás, amelyet a 1139/2013. (III. 21.) Korm.határozat rögzít. A Stratégia az Alaptörvényünkkel összhangban Magyarország biztonságának kialakítása a kibertérben. Ahogy az fizikailag meghatározható határaink védelme esetében, úgy a magyar kibertér védelme is kiemelkedően fontos. A Stratégia tartalmazza többek között a nemzeti adatvagyonunk megfelelő védelmét és a létfontosságú rendszerlemek informatikai hálózatának megóvását a támadásokkal szemben.

2.1. Fenyegetés, kiberfenyegetés

Az adatvagyonnal kapcsolatos veszélyek megértéséhez szükséges előbb a fenyegetés (minatio) általános fogalmát megismerni: bizonyos hátrányok jogtalan okozásának kilátásba helyezése⁴. Az idegen szavak és kifejezések szótára szerint pedig: „*súlyos hátrány kilátásba helyezése, amely alkalmas arra, hogy a megfenyegetettben komoly félelmet keltsen*”⁵. Ugyanakkor az alábbi felsorolásból érzékelhető, hogy a kibertérből származó támadások, veszélyek bár sokkal komolyabbak, köszönhetően annak, hogy a kibertér egy (fizikai) határok nélküli tér, amely lehetővé teszi többek között a fenyegetések látenciában maradását és a határokon átívelő támadások nemzetközi jellegének megteremtődését.

A kibertérből származó és a nemzeti adatvagyonot fenyegető és veszélyeztető támadásokat az alábbi felosztásba sorolom:

- a fizikai támadás, amely valamilyen fizikai erőszakkal történő adatszerzést jelent,
- social engineering vagy emberek (értsd alkalmazottak) befolyásolása,
- hardveres támadás, ilyen pl. a keylogger alkalmazása,
- szoftveres támadás, amikor az adatszerzéshez valamilyen rosszindulatú szoftvert vagy programot használnak fel.

A kibertámadások célja lehet információszerzés, és ezáltal akár pénzszerzés zsarolással vagy befolyásolással; úgynevezett erődemonstráció vagy politikai célok; a megtámadott fél vagy annak környezete félelemben tartása stb.

Az említett támadási formák megvalósulhatnak önállóan, de akár vegyesen is, függően az elkövetők tapasztalataitól, taktikájától és a megszerzendő információk védettségétől.

⁴ www.kislexikon.hu (Letöltés ideje: 2017. 10. 27.)

⁵ BAKOS Ferenc: Idegen szavak és kifejezések szótára, Akadémia Kiadó Budapest 2002.

3. A nemzeti adatvagyon és Magyarország egyes „kiberszervezetei”

A következőkben az olyan hazai szervezetek feladatait kívánom bemutatni, amelyek jogszabályi felhatalmazás alapján elhárítja és kezeli a kibertérből érkező fenyegetéseket és a nemzeti adatvagyon kezelésével, védelmével összefüggésben látnak el feladatokat.

3.1. A Magyar Honvédség feladata a kibertérben

Ahogy Kovács László mk. ezredes rámutatott, a kiberhadviselés célpontjai lehetnek akár a szembenálló fél információs rendszerei (ilyenek a katonai-, közigazgatási- és nemzetbiztonsági rendszerek), akár a kritikus információs infrastruktúrák (energiaellátás, ipari irányítás, kommunikáció, közlekedés stb.)⁶ Ehhez a megállapításhoz annyit tennék hozzá, hogy a XXI. században már rájöttek arra, hogy az aragnál is értékesebb az információ vagy adat – amelynek feketepiaci értéke magasabb is lehet – így akár az államok egymás föléti befolyásolásának, uralmának megteremtése nemcsak fizikai értelemben történhet meg, hanem a kibertérből érkező támadásokkal is, amelyek akár csak időlegesen is, de lebéníthatják az adott állam infrastruktúráját, működését.

Emiatt érdemes kiemelni a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról szóló 60/2013. (IX. 30.) HM utasítás megállapítását, mivel az külön kitér az információs fenyegetésekre, valamint utal a korábban bekövetkezett eseményekre, mint például a 2007-es Észtországot érő orosz kibertámadás, amelyet követően megváltozott a világ gondolkodása a háborús konfliktusok helyszínéről. Az utasítás már nyíltan kimondja, hogy az iráni urándúsítót ért vírustámadás kiberháborúként értelmezhető⁷.

„A fenyegetett célok változnak, egyre szélesebb körű szolgáltatások veszélyeztethetők. A támadó célja infokommunikációs eszközök alkalmazásával a vezetési és irányítási rendszerek feletti irányítás megszerzése, a támadott fél erőinek lekötése, reagáló képességének felmérése, a nemzeti kritikus infrastruktúrák, a nemzeti adatvagyon veszélyeztetése vagy a katonai műveletek, katonai erő hatékony alkalmazásának blokkolása, befolyásolása. ...A támadás forrása lehet hacker tevékenység, szervezett bűnözés, ideológiai vagy politikai szélsőség, kormányzati támogatással rendelkező agresszió.”⁸

A Magyar Honvédség alapvető feladata Magyarország függetlenségének, területi épségének és határainak katonai védelme, nemzetközi szerződésből eredő közös védelmi és békefenntartó feladatok ellátása, valamint a nemzetközi jog szabályaival összhangban humanitárius tevékenység végzése.⁹

⁶ Prof. Dr. Kovács László mk. ezredes Ludovika Szabadegyetem előadása 2015. március 24-én

⁷ Stuxnet vírus: 2010-ben az iráni Bushehr erőműben urándúsítója elleni számítógép-vírussal fertőzött támadás, amelynek következtében az urándúsítóban üzemzavar, illetve leállás következett be.

⁸ 60/2013 (IX. 30.) HM utasítás

⁹ <http://www.kormany.hu/hu/mo/honvedelem> (Letöltés ideje: 2017. 10. 27.)

A honvédelem nemzeti ügy¹⁰. A Magyar Honvédség részére a honvédelmi miniszter a 60/2013. (IX. 30.) HM utasításban a következő általános célkitűzéseket határozza meg:

- a) *katonai kritikus információs infrastruktúrák elleni támadás elhárítása;*
- b) *katonai kritikus információs infrastruktúrák sebezhetőségének csökkentése;*
- c) *katonai kritikus információs infrastruktúrák sérüléseinek helyreállításához szükséges idők csökkentése;*
- d) *honvédelmi célú feladatvégrehajtás szempontjából a kritikus információs infrastruktúrák védelmének biztosítása kapcsán az ágazati együttműködési feladatok végzése, részvétel a nemzeti kritikus infrastruktúra védelmi programokban és feladatokban, a katonai kritikus információs infrastruktúra védelem továbbfejlesztése a honvédelmi kritikus információs infrastruktúra-védelem irányába.”¹¹*

Magyarország (is) rendelkezik katonai stratégiával¹², amelyben a kiberteret új kihívásként és potenciális veszélyforrásként jellemzi, és amelyben Magyarország számára is fenyegetést jelentenek a megnövekedett számú számítógépes támadások, emiatt szükségesnek érzik a háború fogalmának újraértelmezését. Továbbá globális kihívásként értékeli, hogy ennek köszönhetően a kibertérből érkező fenyegetésekre adott válaszreakció és döntéshozatali idő megrövidül a korábbiakhoz képest.

Álláspontom szerint az egyre jobban megszorodó kibertámadások miatt a Magyar Honvédség feladatai szélesedtek, mivel nemcsak a határaink védelmében, a szövetséges fegyveres erők támogatásában szükséges a részvételük, hanem a digitális kihívás következtében és annak hatásaként kiemelten fontos feladatuk van tekintettel a NATO 5. Cikkelyére és annak változásaira, hogy a szükséges mértékben megvédjék Magyarországot az esetleges kibertérből érkező fenyegetésekkel szemben, amelyek veszélyeztethetik nemcsak az ország függetlenségét, hanem az állampolgárok biztonságát is.

3.2 A Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat feladatai a nemzeti adatvagyon és kritikus információs infrastruktúrák védelme esetében

Az információs társadalom egyes elemei közül a honvédelmi ágazatot érintő szabályozást tekintetem át. A honvédelmi célú elektronikus információs rendszerre vonatkozó szabályok legalább hét jogszabályban (törvény és kormányrendelet) fogalmazódtak meg és módosításra is kerültek. Az ágazati jogalkalmazók feladata tehát nem egyszerű, nem csak a keletkezett joganyag száma miatt, hanem a jogszabályok a hatáskör gyakorlójának jogosultsága vagy kötelezettsége tekintetében történő összevetése és értelmezése miatt is.

¹⁰ 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

¹¹ 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójáról, 1. sz. melléklet 7.2. 1) pont.

¹² 1656/2012 (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról

A honvédelmi célú elektronikus információs rendszer fogalmát¹³ kormányrendelet határozza meg az Ibtv.¹⁴ felhatalmazása alapján. Megállapíthatóan ez az információs rendszer összetett, mivel a honvédelemért felelős miniszter vezetése, irányítása alatt álló szervek zárt célú elektronikus információs rendszereit, valamint egyéb – funkciójára, rendeltetésére, feladatellátására szerint – nyílt elektronikus információs rendszereit jelenti. A két információs rendszer összessége támogatja ágazat-specifikus módon a honvédelmi ágazaton belüli és ágazatok közötti működést.

A honvédelmi ágazatban is a zárt célú elektronikus információs rendszer a rendeltetése szerint elkülönült információs rendszer, amely információs feladatok ellátását biztosítja, és kizárólagosan specifikus igények kielégítését szolgálja az a célra létrehozott szervezet útján és működése által. Ez utóbbiak a honvédelemért felelős miniszter vezetése, irányítása alá tartozó szervek és a tulajdonosi joggyakorlása alatt álló gazdasági társaságok használatában lévő zárt célú elektronikus információs rendszereket jelentik, amilyenek a honvédelmi célú közigazgatási döntés-előkészítő és vezetés-irányítási rendszerek, a honvédelmi stacioner és táborigazgatási műveleteket, valamint gyakorlatokat támogató műveleti vezetési rendszerek, a katonai nemzetbiztonsági területen titkos információgyűjtést, illetve titkos adatszerzést támogató rendszerek.¹⁵

A zárt célú elektronikus információs rendszerek egyszerűsítetten a következőkben tagolandók (a titkos információgyűjtést ettől elkülönítve):

- a Magyar Honvédségnél üzemelő MH Kormányzati Célú Elkülönült Hálózat (katonai és közigazgatási szakfeladatok), amely a honvédelmi szervezetek központi szolgáltatásait látja el – mellette rengeteg helyi rendszer üzemel; valamint a KNBSZ¹⁶ elkülönült hálózata;
- a védelmi igazgatási szakfeladatokot szolgáló rendszer;
- a HM tulajdonú gazdasági társaságok saját rendszerei.

Az említett szakfeladatokat integráltan a következő ábra szemlélteti (mint ágazati és a KNBSZ szervezeti feladatok ellátása). Az első pillér: eseménykezelés (ágazati és KNBSZ saját), a második pillér: sérülékenységvizsgálat (honvédelmi célú elektronikus információs rendszereknél), a harmadik pillér: elektronikus információbiztonsági felügyeleti és hatósági feladatok ágazati szinten:

¹³ 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 1. § 2.

¹⁴ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1.§ 47.

¹⁵ 15/2017. (IV.28) HM utasítás a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól

¹⁶ Katonai Nemzetbiztonsági Szolgálat.



1. ábra¹⁷

A honvédelmi elektronikus információs rendszerekkel összefüggésben szükséges kiemelni KNBSZ nemzetbiztonsági feladatai közül a kibertér biztonságára vonatkozókat, úgy mint az információk gyűjtését a honvédelmi érdeket veszélyeztető kiber-tevékenységről és szervezetekről, valamint a honvédelemért felelős miniszter által vezetett minisztérium, a Honvéd Vezérkar információvédelmi tervező munkájához szükséges adatok biztosítását¹⁸. Ezen feladatai ellátása során a KNBSZ elemzi és értékeli a működési területén felderített, a nemzetbiztonság katonai elemeit érintő információkat, azokról folyamatosan tájékoztatja a honvédelemért felelős minisztert, a minisztérium feladat- és hatáskörrel rendelkező vezetőit, a Magyar Honvédség feladat- és hatáskörrel rendelkező parancsnokait, vezetőit, a vezérkari főnököt, valamint a főparancsnokot.¹⁹

A honvédelmi ágazatnál (EU terminológiával: szektornál) a kibertér védelmét – zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátását, továbbá a honvédelmi célú elektronikus információs rendszerek biztonságának felügyeletét – kizárólagosan a KNBSZ látja el (a KNBSZ főigazgatója a nevesített, mint Kormány által kijelölt hatóság²⁰). Tehát az ágazatspecifikusságra tekintettel a kibervédelemben a szervezet a jogosult és kötelezett a korábban már összetett jelzővel illetett elektronikus információs rendszerek vonatkozásában, így a kormányrendelet azonos jogszabályhelyeket jelölt meg a feladatellátásában.

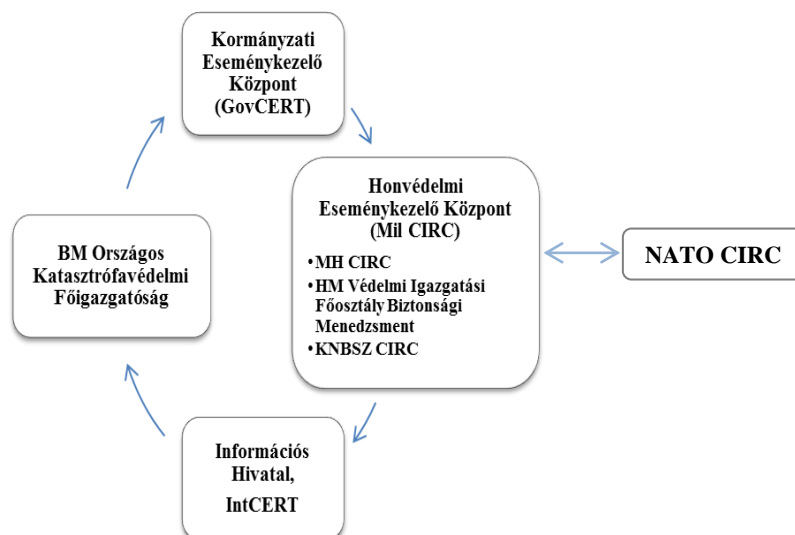
A honvédelmi ágazati eseménykezelésben együttműködés van (következő ábra szemlélteti), az azonosított szereplők mellett az Alkotmányvédelmi Hivatal, a KKM és a nemzeti koordinációs feladatokat végző nemzeti kiberkoordinátor említendő még. Az eseménykezelési együttműködés egyben a honvédelmi ágazat nemzeti és nemzetközi szervezetekkel való kapcsolati rendszerét is megmutatja. A KNBSZ szakmai felkészültsége biztosíték adott kibervédelmi területű művelet (pl. egy kód elemzése) vagy stratégia szintű feladat megoldásához szükséges közös kormányzati szintű együttműködéshez (pl. munkacsoportban egy folyamat kidolgozása, jogszabály előkészítése).

¹⁷ Az ábra Dr. Kassai Károly ezredes: Honvédelmi célú elektronikus információs rendszerek címet viselő, a BM OKF-en, 2016. október 26-án, a kiberhónap keretében megrendezésre kerülő előadásának eleme.

¹⁸ 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról 6. § g)

¹⁹ 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról 7. § (1) bekezdés

²⁰ 187/2015 (VII.13.) Korm. rendelet 15. § (2) bekezdés



2. ábra²¹

A KNBSZ, mint kijelölt hatóság elektronikus információbiztonsági felügyeleti feladatait a felsorolás mutatja be:

- ellenőrzés, intézkedés, visszaellenőrzés;
- biztonsági esemény kivizsgálás elrendelése;
- tudatosság növelése;
- kockázatelemzés;
- kibervédelmi gyakorlatok;
- kapcsolattartás;
- nyilvántartás;
- sérülékenységvizsgálat elrendelése.

Kiegészítés a felsoroláshoz a teljesség igénye nélkül:

A kibervédelmi gyakorlatok kettős feladatot jelentenek: az eseménykezelő központ és funkciói végzik a gyakorlati feladatokat, az esetleges kapcsolattartási és egyéb feladatok (pl. együttműködési szerződés) a hatósági feladatok közé tartoznak.

A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események (tehát az elektronikus biztonsági rendszerben változást vagy ismeretlen helyzetet előidéző, nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat stb.), és fenyegetések kezelése a KNBSZ kijelölt szerveinek feladata²², és a szakmai irányítása és koordinálása alatt álló, szakfeladat szerint elkülönülő – a

²¹ Az ábra Dr. Kassai Károly ezredes: Honvédelmi célú elektronikus információs rendszerek című műve, a BM OKF-en, 2016. október 26-án, a kiberhónap keretében megrendezésre kerülő előadásának eleme.

²² 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő – eseménykezelő központokkal együtt látja el.

A magyar eseménykezelés folyamatában a kommunikációs protokoll egyszerű: GovCERT²³ központú, ami azt jelenti, hogy az eseményeket a GovCERT felé kell bejelenteni, aki továbbítja a szükséges információkat az összes érintett szervezet felé, rögzíti az esetet, szükség esetén közvetlen együttműködést ajánl fel.

A KNBSZ részéről²⁴ megfogalmazott vélemény (vélelmezhetően további kibervédelmi szereplők egyetértésével), hogy az Ibtv. és végrehajtására megjelent kormányrendeletek által megfogalmazott elektronikus információbiztonsági követelményrendszer, egy új szakmai kultúra megalapozásának tekinthető. A kibervédelem jogi szabályozásának hatékonysága, működőképessége nemzeti szinten 8-10 év múlva lesz azonosítható, amennyiben a szükséges markerek („bizonyítékok”) gyűjtése és elemzése megtörténik.

Megfogalmazásra került néhány, kifejezetten a jogi szabályozásra vonatkozóan gyakorlati szempontú vizsgálati érdekesség is:

- hogyan kell jó szabályzatot írni (folyamatokat meghatározni) egy közigazgatási szervezetnél;
- a kockázatelemzés szempontjai úgy, hogy azok szervezetek között is értelmezhetők legyenek;
- a biztonsági osztályra vonatkozó egyedi megfogalmazási lehetőségek mennyire támogatják-befolyásolják a nemzeti infrastruktúrák kialakulását;
- a minősített elektronikus adatkezelés és az Ibtv. kapcsolata.

3.3. Nemzeti Kibervédelmi Intézet (NKI)

Az Ibtv. 2015. évi módosításának eredményeként 2015. október 1-jén megalakult a Nemzeti Kibervédelmi Intézet – a Nemzetbiztonsági Szakszolgálat keretei között –, amelyen belül három szakmai szervezeti terület került elkülönítésre a tevékenységüknek megfelelően:

- a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó incidenskezelési szakterület (a Kormányzati Eseménykezelő Központ, azaz a GovCERT);
- a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH);
- a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási és sérülékenységvizsgálati (GovCERT) szakterület.

A három terület mellett az NKI feladata még többek között a honvédelmi és a kritikus információs infrastruktúrák védelme is.

²³ A Kormányzati Eseménykezelő Központ (GovCERT-Hungary) a magyar kormányzat információ-megosztó és incidens-kezelő szervezete. Lásd: <http://www.cert-hungary.hu/node/1> (Letöltés ideje: 2017. 10. 27.)

²⁴ Dr. Kassai Károly ezredes – KNBSZ

A Kormányzati Eseménykezelő Központ (KEK) incidenskezelési terület feladatai:

- „– *Biztonsági események kezelése,*
- *Fenyegetésmenedzsment,*
- *Ügyeleti szolgálat,*
- *Elemzés/értékelés,*
- *Kibervédelmi gyakorlat,*
- *Képzés, tudatosítás,*
- *Felelősök kijelölésének támogatása,*
- *Sérülékenységi vizsgálat,*
- *biztonsági esemény-kezelés kapcsán együttműködés az internet-szolgáltatókkal,*
- *rendszeres vezetői tájékoztatás,*
- *biztonságirányítás és sérülékenységi vizsgálat,*
- *sérülékenységi vizsgálat,*
- *biztonsági események kivizsgálása,*
- *EMIR/FAIR rendszerekkel²⁵ kapcsolatos informatikai biztonsági feladatok ellátása.*”²⁶

A GovCERT alapvető feladata az állami és önkormányzati szervek informatikai biztonsági támogatása,

- amely egyrészt preventív jellegű, (értve ezalatt a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követését és a sérülékenységi menedzsmentet),
- másrészt pedig reaktív jellegű, a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és – több állami szervet érintően - a kezelésük koordinációjára irányul.

A Nemzeti Elektronikus Információbiztonsági Hatóság (NKI) feladatai:

- „– *ügyfelek és rendszerek nyilvántartása,*
- *biztonsági osztályba és szintbe sorolás ellenőrzése,*
- *követelmények teljesülésének ellenőrzése (jogsabályi követelmények és eljárási szabályok teljesítése megtörtént-e),*
- *sérülékenységi vizsgálat elrendelése,*
- *javaslat létfontosságú rendszer kijelölésére,*
- *javaslat információbiztonsági felügyelő kirendelésére,*”²⁷
- *engedélyezések/hozzájárulások,*
- *az Unió tagállamaiban történő elektronikus információs rendszer üzemeltetés tekintetében engedélyezési eljárás lefolytatása.*

²⁵ EMIR/FAIR rendszerek jelentése: Egységes Monitoring és Információs Rendszer/ Fejlesztéspolitikai Adatbázis és Információs Rendszer, amelyek az Európai Unió és Magyarország által finanszírozott pályázati projektek. Célja többek között, hogy egy egységes pályázati felületen lehetséges a pályázatokat kezelni.

²⁶ <http://nbsz.hu/?mid=42> (Letöltés ideje: 2017. 11. 20.)

²⁷ Uo.

A fenti felsorolásból a sérülékenység vizsgálatot²⁸ szeretném kiemelni, mint olyan tevékenységet, amelynek célja az esetleges biztonsági események bekövetkeztét megelőzően az elektronikus információs rendszer gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása. A sérülékenységvizsgálat végrehajtása során a vizsgálat alá vont elektronikus információs rendszerben felkutatásra kerülnek – többek között – a potenciális szoftverhibák, gyenge jelszavak, hibás beállítások, amelyeket a támadó kihasználhat, és ezeken keresztül kárt tud okozni a rendszerben.

Az egyes rendszerek esetében az ismeret ezen foka, a sérülékenységvizsgálat által feltárt információk jellege, nemzetbiztonsági szempontú megközelítést kíván. Az Ibtv. éppen emiatt rendelkezik arról, hogy a zárt célú elektronikus információs rendszerek, az állami és önkormányzati szervek létfontosságú rendszerlemeinek elektronikus információs rendszerei, valamint a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek vonatkozásában kizárólag a GovCERT végezheti a sérülékenységvizsgálatot, kivéve a honvédelmi célú elektronikus információs rendszereket, valamint a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit. A fenti körbe nem tartozó állami rendszerek esetében pedig lehetővé teszi magas szintű szakmai és biztonsági elvárásoknak megfelelő gazdálkodó szervek számára a sérülékenységvizsgálat lefolytatását.

A sérülékenységvizsgálat eredményeként előálló vizsgálati jelentésben a GovCERT minden esetben javaslatot tesz az azonosított sérülékenységek kijavítására is.

Míg az NKI egyes szakterületei kívülről támogatják az állami és önkormányzati szerveket abban, hogy saját rendszereik védelmét ellássák, és ennek keretében kialakítsák saját ún. információbiztonsági irányítási rendszerüket (röviden: biztonságirányítási rendszer), addig a biztonságirányítási szakterület ezt a feladatot tevélegesen is végzi – részint az NKI biztonsági felügyeletére bízott, kiemelt kormányzati rendszerek esetében, részint pedig szakmai támogatást nyújtva a hatósági szakterület részére.

4. A létfontosságú információs rendszerek és rendszerlemek biztonságáról

A létfontosságú információs rendszerlemek, vagy kritikus információs infrastruktúrák biztonsága kiemelten fontos a nemzeti adatvagyon (mint nemzeti vagyon része) megőrzésének érdekében. Ennek biztosítása érdekében az alapvető biztonsági követelményeket meg kell valósítani, így a rendelkezésre állást, a bizalmasságot és a sértetlenséget mind az információs rendszerben tárolt adatokra vonatkozóan mind pedig a magának a az elektronikus információs rendszer és

²⁸ 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és z eseménykezelő központok feladat-és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és sérülékenységvizsgálat lefolytatásának szabályairól 14. § – 20. §-alapján

elemeinek sértetlensége és rendelkezésre állását, a zárt, teljes körű, folytonos és kockázatokkal arányos védelmét²⁹.

Az Lrtv. végrehajtási rendelete alapján szakhatóságként első fokon a BM OKF helyi, míg másod fokon a területi szerv van kijelölve.³⁰

A törvény mellett számos olyan végrehajtási rendeletet alkottak, amelyek meghatározzák a kritikus infrastruktúrákkal kapcsolatban a létfontosságú rendszerek és létesítmények azonosítását, kijelölését és védelmét. Ilyen végrehajtási rendelettel történik például az infokommunikációs technológiák ágazathoz tartozó létfontosságú rendszerelemeket, az egészségügyi létfontosságú rendszerelemeket, az energetikai létfontosságú rendszerelemeket, az agrárgazdasági rendszerelemek és létesítmények, vízgazdálkodási és vízi létesítményeket és a rendvédelmi szerveket és a Rendőrséget érintő szabályozás.

A létfontosságú rendszerelemek, ahogy fentebb említettem, érintettek az adatvagyon megőrzésében és védelmével kapcsolatban. Ebben a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (továbbiakban: LRLIBEK) által végzett feladatok fontos szerepet játszanak.

4.1. LRLIBEK tevékenysége

Az LRLIBEK, mint ágazati kijelölő szakhatóság hatósági feladatai a fent említett biztonsági osztályba szintbe sorolás, a követelmények ellenőrzése, hiányosságok elhárítása, kockázatelemzés végzése, a biztonsági eseményekkel kapcsolatos bejelentések vizsgálata, a kapcsolattartás és együttműködés biztosítása³¹. A felsoroltakon kívül az LRLIBEK eseménykezeléssel kapcsolatos feladatai³² a tudomásra jutott biztonsági eseményekről történő értesítés, szakmai támogatás nyújtása, a sérülékenységgel és a fenyegető kockázatokkal kapcsolatban a hatóságok és az eseménykezelő központok támogatása, éves jelentés készítése, ajánlások, állásfoglalások kibocsátása, oktatói, szakértői tevékenység elvégzése.³³

5. Kiberbiztonság fejlesztése a tudatosság növelésével:

A kibervédelem leghatékonyabb módja a biztonságtudatosság bevezetése, úgy, hogy az információs rendszereket használó, az azokkal rendelkező személyeket megfelelő oktatásban, képzésben részesítsék annak érdekében, hogy azok ismeretében tudatosan végezzék a feladataikat. A tudatosság növelésének szükségességét az oktatásban és a folyamatos képzésekben látják megvalósíthatónak például a Belügyminisztérium vagy Magyarország egyes egyetemei, így a Nemzeti Közszolgálati Egyetem is. A hazai állami elektronikus biztonsági rendszerek vonatkozásában a teljes körű biztonsági szint eléréshez, a kielégítőnek tekinthető

²⁹ 2013. évi L. törvény 5.§ (a)-(b) bekezdései

³⁰ 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról 4.§ (2) bekezdés

³¹ 2013. évi L. törvény 20.§ c.)-m.)

³² 185/2015. (XII. 13.) Korm.rendelet

³³ Ibtv. 4. § a., 5. § 2)-3) bekezdése

kiberbiztonság megteremtéséhez nem elegendő az optimálisnak tekinthető szervezetrendszer kialakítása, új technológia bevezetése és alkalmazása. Amennyiben az anyagi erőforrások nem biztosítják a már meglévő és biztonságilag hiányos rendszereknek az Ibtv.-ben meghatározott, a biztonsági szint emelését előíró folyamatokat, nem lehet a kibervédelem sikerességéről beszélni, illetve azt elvárni.

A tudatosító tevékenység számos réteget céloz, ezek közt elsősorban kell említeni a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését, és tőlük várható el a védelmi intézkedések működtetése), és a felhasználókat, akiket meg kell tanítani az internet és az információs technológiák biztonságos használatára, saját és rájuk bízott adatok felelős és szakszerű kezelésére.

A nemzeti adatvagyon védelméről szóló 2010. évi CLVII. törvény alapján nemzeti adatvagyonnak minősül a „közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.”³⁴

A Fehér Könyv tanulmányában a fogalmi megközelítés alapján külön veszi a közszférát és a magánszférát, mely utóbbival bár szükséges lenne foglalkozni, de a törvény mégsem teszi ezt meg.

Az állami szférával kapcsolatban megkülönbözteti az állami szervek és vállalatok, valamint az önkormányzati szervek és vállalatok révén létrejövő adatokat, így a különböző nyilvántartásokat, jogi- és szervezeti normákat, gyűjteményeket, stb.³⁵

6. Az Európai Unió Kiberbiztonsági Stratégiája

Az Európai Unió kiberbiztonságának megteremtését sürgető stratégiájába fogalmazta meg azt az 5 prioritást, amelynek egyes elemei honvédelmi feladatnak minősíthető:

- „– a kibertámadásokkal szembeni ellenálló képesség elérése,
- a számítástechnikai bűnözés drasztikus csökkentése,
- kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében,
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése,
- összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió alapértékeinek támogatására.”³⁶

A felsoroltakból a tanulmány szempontjából a KBVP feladatok ellátását emelem ki egy rövid gondolat erejéig, mivel ebben fejezi ki az Unió szándékát arra

³⁴ 2010. évi CLVII. törvény 1. § 1.) pontja

³⁵ Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér Könyvhöz (Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete Budapest, 2016. július p.19.)

³⁶ Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az Európai Unió kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér, Brüsszel, 2013.2.7. JOIN(2013) 1 final, <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001> (Letöltés: 2017. 10. 27.)

vonatkozóan, hogy fejlesszék a tagállamok a kommunikációs és információs rendszerek védelmére irányuló képességét. Ezek a fejlesztések a civil és a katonai módszerek közötti együttműködésre kell, hogy irányuljanak, amire történő törekvés hazánkban is megindult a jogi szabályozás tekintetében, ugyanakkor a már többször említett Ibtv-t és annak végrehajtási rendeletét továbbá a KI-re vonatkozó törvényt leszámítva, azzal nem foglalkoznak érdemben a jogalkotók.

A nemzeti adatvagyon védelmével kapcsolatban az Unió Stratégiája külön nem tesz említést.

7. Összegzés

A nemzeti adatpolitikáról szóló Fehér Könyv – amit a Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testületének (továbbiakban Testület) 2016 júliusában kiadott tanulmánya – nyitó gondolatát idézve, a „gazdaság új hatóanyaga az adat”. Az adat szabályozásával kapcsolatban a Fehér Könyv levezeti azt a stratégiát – nagyon helyesen – ami az adatpolitika kialakításával kapcsolatban szükséges és amelynek a Testület szerinti kialakítása javasolt (figyelembe véve, hogy hazánkban jelenleg nincs kialakított védelem).

Figyelembe véve az említett jogszabályokat és a Fehér Könyv álláspontját, logikátlanok találok, hogy a nemzeti adatvagyonra csak és kizárólag, szigorúan értelmezve állami-, illetve önkormányzati szervezetek és vállalatok kezelhetnek, míg a magánszférához tartozó vállalatok, egyetemek, magánszemélyek által kezelt adatok – amíg nem kerülnek az állami szférába – addig a törvény szerint nem minősül nemzeti adatvagyonnak és nem részesül védelemben?! Vagyis ugyanannak az adatnak a védelme kizárólag az adat kezelőjének jogi szabályozásban megítélt szerepétől függ? Miközben a magánszektorhoz tartozó vállalatok információs rendszerein keresztül ugyanúgy és sokszor ugyanazokat az adatokat kezelik. Így felmerül a kérdés, hogy az adatokat kezelő szervezetek között – beleértve az állami- és a magánszektor is – szabad-e ugyanazon tényezők tekintetében eltérő szabályozással különbséget tenni, és ha igen, akkor a hasonló vagy éppen ugyanazon adatok esetében a különböző regulációk nem vezethetnek-e visszaéléshez.

Álláspontom szerint éppen azért, mert a kibertér számtalan lehetőséget rejt, mind jó és rossz értelemben, a Mavtv³⁷. által nevesített, minősített adatok tekintetében szükséges az azonos szintű védelem.

Zárásképpen egy másik érdekesség ezzel kapcsolatban, mely jelenleg még nyitott kérdés, hogy a 2018. május 25-én életbe lépő az Európai Unió általános adatvédelmi rendelete, a GDPR (General Data Protection Regulation) szabályozása mellett – ami nemcsak az állami szervekre, hanem a KKV-kra, valamint a jogi személyiséggel nem rendelkező gazdasági társaságokra és az állampolgárokra is vonatkozik – mennyire tud érvényesülni a Nyilvántartási törvény néven ismert, a nemzeti adatvagyon körébe tartozó nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény.

³⁷ 2009. évi CLV. törvény a minősített adat védelméről

Felhasznált irodalom:

- 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának Kiadásáról
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)
- Megalapozó tanulmány a nemzeti adatpolitikáról szóló Fehér Könyvhöz (Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete)
- 1656/2012 (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról
- 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről
- 278/2011. (XII. 20.) Korm. rendelet a NATO Válságreakálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről
- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
- Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Unió kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér /2013/01 final (forrás: EUR-lex-52013JC0001-EN-EUR-Lex)
- Zöld Könyv A létfontosságú infrastruktúrák védelmére vonatkozó európai programról, COM(2005) 576 final, Európai Bizottság Brüsszel, 2005. 11. 17.) <http://ec.europa.eu/transparency/regdoc/rep/1/2005/HU/1-2005-576-HU-F1-1.Pdf> (Letöltés ideje: 2017. 10. 27.)

A RACIONÁLIS GONDOLKODÁS KÉPESSÉGÉNEK KVANTITATÍV MÉRÉSE

BEVEZETÉS

Legtöbbünk találkozott már olyan személyekkel, akik tagadhatatlanul igen intelligensek, műveltek és tanultak voltak, mégis rendszeresen ostobaságnak tűnő dolgokat beszéltek, irracionálisan viselkedtek, vagy igazolhatóan téves nézeteket vallottak. Nem ritka az sem, hogy ez az „okos, de butaságokat csinál” jelenség tartósan kimutatható egy személy viselkedésében, komoly döntéseiben is megmutatkozik, s így kihat a személy magánéletére és szakmai pályafutására is.

Az „okos, de butaságokat csinál” nyilván köznyelvi megfogalmazás, amelyet a mélyebb vizsgálathoz pontosítani szükséges. Ismeretelméleti szempontból megfogalmazva, általánosan megfigyelhető, hogy az emberek:

- rosszul mérik fel a valószínűségeket,
- nem hatékonyan tesztelnek különböző feltételezéseket,
- nem látják világosan saját hitrendszerük, előzetes meggyőződéseik befolyásoló erejét aktuális döntéseikben,
- választásaikban komoly szerepet játszanak lényegtelen információk, miközben lényeges információkat figyelmen kívül hagynak,
- nem vesznek figyelembe lehetséges alternatív magyarázatokat, amikor adatokat értékelnek,
- döntéelméleti hibákat vétének,
- valamint számos egyéb különböző információ-feldolgozási hibát is elkövetnek.

E jelenség pontosabb megértéséhez e cikk az „intelligencia” és a „racionalitás” fogalmi konstruktumát speciális és pontosabb megvilágításban fogja tárgyalni. Szó lesz a racionális gondolkodást rongáló kognitív torzításokról, valamint a cikk bemutatja a racionális gondolkodási képesség kvantitatív mérésének legújabb eredményeit is.

1. A RACIONALITÁS MÉRÉSÉNEK ELMÉLETI HÁTTERE

1.1. Az intelligencia tágabb és szűkebb értelmezése

A kognitív torzítások pszichológiai és ismeretelméleti fogalmának pontos megértéséhez szükség van az intelligencia és a racionalitás fogalmának – minimálisan e cikk tekintetében érvényes – pontosítására.

Az intelligencia szó a latin „intelligentia” szóból ered és a XIV. század óta használatos. Az intelligencia fogalma egyaránt megjelenik a köznyelvben és több

tudományterület szaknyelvében is, de a fogalom definíciója mégsem annyira világos, mint az a használat gyakoriságából következne.

Az intelligencia tágabb definícióiban – még pontosabban a fogalmat tágabban értelmező elméletekben¹ – az intelligencia tartalmi elemei nagyjából megfelelnek annak, amit a köznyelv is ért a fogalom alatt. Ilyenek a „környezethez való alkalmazkodás képessége”, a „problémamegoldó képesség”, a „bölcesség”, a „kreativitás”, a „okosság”, az „ismeretekkel való rendelkezés”, illetve ehhez hasonló bizonytalanul körvonalazott és definiált képességek függetlenül attól, hogy a jelenleg használatos intelligencia tesztek valóban mérik-e ezeket a képességeket vagy sem.

Az intelligencia szűkebb definíciója, illetve elmélete pragmatikus szempontból közelíti meg az intelligencia fogalmát és azt leszűkíti arra a képességre (vagy azokra a képességekre), amit az általánosan használt intelligencia tesztek valóban mérnek. Ennek a pontos megfogalmazása szintén nem egyszerű feladat, de konszenzus látszik kialakulni abban, hogy ez a képesség a kognitív „bontás”, vagy „szétkapcsolás² képessége”, ami a másodlagos – tehát a világ konkrét érzékelésétől elválasztott – mentális reprezentációkkal történő egyszerű, vagy bonyolultabb mentális műveletek végzésének képességét jelenti.

Amennyiben az intelligencia tágabb definícióját használjuk, akkor a felvetett „okos, de butaságokat csinál” probléma feloldásához nem kerülünk közelebb. Minél több kognitív képességet értünk bele az intelligencia fogalmába, annál nehezebb lesz magyarázatot adni arra, hogy egy intelligens személy, birtokában mindezen kognitív képességeknek, miért hoz esetleg sorozatosan rossz döntéseket. Nem világos, hogy miért szuboptimális a gondolkodása, ha megvannak azok a képességei (ismeretek, bölcesség, kreativitás stb.), amelyek elvileg pontosan arra tennék képessé, hogy helyes döntéseket hozzon.

Ilyen típusú paradoxonnal nem találkozunk, ha az intelligencia szűkebb definícióját használjuk. Ebben az esetben az intelligencia csak egy a kognitív képességek közül. És valóban, a tapasztalat azt mutatja, hogy az intelligencia teszteken magasabb értéket elérő személyek ugyanúgy hajlamosak téves gondolkodásra, mint azok, akik átlagos értékeket érnek el. Ebből viszont egyszerűen csak az következik, hogy a tesztek által mért intelligencia képessége nem az egyetlen, sőt, talán nem is a legfontosabb elem az ilyen típusú téves gondolkodás elkerülésében. Keith Stanovich amerikai pszichológus meggyőző érveket sorakoztat fel amellett, hogy a „racionalitás”, a racionális gondolkodás képessége – illetve annak hiánya – az a faktor, amely a vizsgált „okos, de bután cselekszik” jelenség mögött meghatározóan feltűnik³.

¹ Mint például a népszerű Cattell–Horn–Carroll elmélet, amely talán a legbefolyásosabb elmélete az intelligenciának. Lásd: FLANAGAN, Dawn, P - DIXON, Shauna G (2014): The Cattell-Horn-Carroll Theory of Cognitive Abilities

² Cognitive decoupling

³ STANOVICH, Keith E (2009): What Intelligence Tests Miss: The Psychology of Rational Thought, Yale University Press p. 8.

1.2. A racionalitás fogalma

A szintén latin gyökerű „racionalitás” vagy a „racionális” jelentését az értelmező szótárak meglehetősen általános, köznyelvi formában határozzák meg⁴. A racionalitásnak a kognitív folyamatban játszott szerepének világos megértéséhez a fogalom ennél pontosabb definíciójára lesz szükségünk.

A racionalitást e gondolatmenet folyamán „episztemológiai” vagy „ismeretelméleti” racionalitásként fogjuk definálni. Az *ismeretelméleti racionalitás* azt mutatja meg, hogy valakinek a világról alkotott nézet- vagy vélekedési rendszere mennyire tükrözi a világ valóságosan létező struktúráját. Amennyiben egy személy nézetrendszere számottevően eltér az ismeretelméleti optimumtól (azaz a világot nem az objektív valóságnak megfelelően látja), akkor dacára az esetlegesen magas intelligenciának (azaz a kognitív szétválasztás képességének) a gondolkodása elkerülhetetlenül szuboptimális lesz és hibákkal fog járni.

Ezt a jelenséget nevezzük *diszracionalitásnak*⁵, tehát amikor valaki, noha megfelelő intelligencia-szinttel rendelkezik, mégsem képes a racionális gondolkodás követelményeinek megfelelni. A diszracionalitás egy átfogó fogalom, amely számos olyan, egymástól különböző gyökerű jelenséget takar, amelyek számottevően gátolják az egyént koherens és a világ struktúráját híven tükröző nézetrendszer kialakításában és fenntartásában, illetve – ebből fakadóan – optimális döntési mintázatok használatában.

1.3. Intelligencia és racionalitás

Igen figyelemreméltó, hogy jelenlegi ismereteink szerint a racionális gondolkodás képessége és a mért intelligencia szintje csak gyenge-közepes korrelációt mutat. Mégis, amikor intelligenciáról beszélnek (szakértők és laikusok egyaránt), akkor általában a fogalom tág értelmezését használják – azaz beleértik például az adaptív döntéshozatal képességét is, ami a racionalitás egyik alapvető eleme – miközben az általánosan használt intelligencia-tesztek semmi ilyesmit nem mérnek.

Az intelligencia mérésének nagyjából százéves, a nyugati társadalmak által általánosan elfogadott hagyománya van⁶. Az intelligencia teszteket széles körben használják különböző intézmények kiválasztási folyamataiban az oktatás és a munka világában is. Az IQ tesztek megbízható, gyorsan és könnyen használható eszközöknek számítanak. Ezekben a társadalmakban az intelligencia, mint egy lényeges személyes képesség koncepciója nemcsak elfogadott, hanem igen magasra értékelt tulajdonság is. A magas IQ (Intelligence Quotient – intelligencia-hányados)

⁴ Ésszerű, értelmes, célszerű, józanul gondolkodó stb.

⁵ STANOVICH (2009) p. 18.

⁶ Az első használható intelligencia tesztet Alfred Binet és Theodore Simon francia pszichológusok készítették a francia Oktatási Minisztérium megbízására 1904-ben (Binet-Simon teszt). Az IQ (Intelligencia-hányados, Intelligence Quotient, Intelligenzquotient) kifejezést William Stern német pszichológus és filozófus használta először 1912-ben, a „Die psychologischen Methoden der Intelligenzprüfung: und deren Anwendung an Schulkindern” (Az intelligencia mérésének pszichológiai módszerei és azoknak alkalmazása iskoláskorú gyermekek esetében) című könyvében.

csaknem általánosan vágyott tulajdonság, amely a szakmai sikeresség, s általában az életben történő boldogulás egyik igen lényegesnek vélt záloga is.

Ezzel szemben a racionalitás itt felvázolt, az ismeretelméletből eredeztetett koncepciója csaknem tökéletesen ismeretlen a társadalomban. A szakértők természetesen ismerik a racionalitást csökkentő gondolkodási mintázatokat, de ezeknek kvantitatív mérésére eddig nem létezett módszer, így annak értelemszerűen semmilyen hagyománya nincs. Ebből fakad az a tény, hogy társadalmunk az intelligenciát túlértékeli, a racionalitást viszont nem ismeri, vagy legjobb esetben is alulértékeli. A valóságban az intelligencia és a racionalitás egymást kiegészítő, de külön-külön értelmezendő és mérhető kognitív képességek, amelyek külön-külön is meghatározó módon befolyásolják a gondolkodás hatékonyságát.

2. KOGNITÍV TORZÍTÁSOK

2.1. A kognitív torzítások fogalma

Kognitív torzításnak nevezzük azokat a szisztematikus és visszatérően megjelenő gondolkodási mintázatokat, amelyek a gondolkodást eltérítik az ismeretleméleti optimumtól, másképpen megfogalmazva, a kognitív torzítások szisztematikus és visszatérően jelentkező hibás gondolkodási mintázatok. A fogalmat a Nobel-díjas Daniel Kahneman⁷ és munkatársa, Amos Tversky használta először 1972-ben.

A kognitív torzítások számát nehéz megbecsülni⁸, de jelenlegi 130-150 gyökerükben sokszor erősen eltérő és meglepő változatosságot mutató kognitív torzításról beszélhetünk. Természetesen senki nem produkálja az összes kognitív torzítást, de gyakorlatilag minden ember gondolkodásában fellelhető pár torzítás, akár tudatában van az illető ennek, akár nem.

A kognitív torzítások felelősek a gondolkodás eltérítéséért az ismeretleméleti optimumtól, más szóval a racionális gondolkodástól. Minél több kognitív torzítás jelenik meg valakinek a gondolkodásában, annál kevésbé racionális az illető gondolkodása, függetlenül az intelligencia szintjétől.

2.2. Két típusú gondolkodás

A kognitív torzítások gyökerének pontosabb megértéséhez az emberi gondolkodás mélyebb, evolúciós-pszichológiai megvilágítására van szükség. Jelenlegi tudásunk szerint gondolkodásunk két, egymástól lényegileg különböző rendszeren keresztül történik.

⁷ Daniel Kahneman izraeli-amerikai pszichológus 2002-ben kapta meg a közgazdasági Nobel-díjat (kollégájával Amos Tversky-vel közösen) a viselkedési közgazdaságtan területén végzett meghatározó munkásságáért. A tudományterület növekvő jelentőségét és előtérbe kerülését mutatja, hogy 2017-ben az amerikai Richard H. Thaler kapott közgazdasági Nobel-díjat ugyanezen a területen végzett munkájáért.

⁸ A kognitív torzításoknak egyelőre nem létezik egységesen elfogadott kategorizálása és csoportosítása. Különböző források eltérő osztályozásokat használnak, egybevonnak, esetleg külön említenek olyan torzításokat, amelyek más források másképpen rendszereznek.

<u>1. típusú gondolkodás</u>	<u>2. típusú gondolkodás</u>
gyors	lassú
automatikus	kontrollált
alacsony erő kifejtést igényel	nagy erő kifejtést igényel
asszociációs	szabályokon nyugvó
nem verbális	nyelvi alapú
alapértelmezett	felülíró típusú
nem logikus	logikus
evolúciós szempontból régi	evolúciós szempontból új
párhuzamos szervezésű	soros szervezésű

1. ábra⁹

Az „1. típusú gondolkodás” egy gyors, automatikus, emocionálisan színezett, sztereotipikus, heurisztikus, intuitív és a legtöbb esetben nem tudatosuló gondolkodás. Jó példa az 1. típusú gondolkodásra az arcfelismerés, vagy a mélység érzékelése, mert mindkettő gyors, nem tudatos, hanem automatikus és előző tapasztalatokon alapuló kognitív művelet. Az 1. típusú gondolkodás viszonylag alacsony terhet jelent az agy számára, amiből két igen lényeges következmény is adódik. Az első, hogy az alacsony kapacitás-szükséglet miatt az ember párhuzamosan több 1. típusú gondolkodási műveletet is képes „futtatni” egyidejűleg¹⁰. A második, hogy – nem utolsósorban pont e lehetőség miatt – az 1. típusú gondolkodásunk alapállapota, alapesetben ez a gondolkodás indul el, ha kognitív feldolgozásra van szükség.

A „2. típusú gondolkodás” viszonylag lassú, az agy számára nagy leterheléssel járó, tudatos gondolkodási művelet. 2. típusú gondolkodást használunk, ha olyan helyzetbe kerülünk, amikor koncentrált, lépésről lépésre történő, módszeres és tudatos gondolkodásra van szükségünk, például, ha egy nehezebb matematikai feladványt oldunk meg. A koncentráció-igény, a nagy kapacitás-szükséglet miatt az 2. típusú gondolkodás soros jellegű, azaz nem igazán tűr meg maga mellett párhuzamos gondolkodási folyamatokat.

Az 1. és 2. típusú gondolkodás világos, evolúciós alapokon nyugvó munkamegosztásban dolgozik. Az 1. típus az evolúciós szempontból régi, bevált feldolgozási rendszerünk, amely figyelemreméltóan hatékony munkát végez a mindennapi élet során. Gyors, alacsony erő kifejtést igénylő, párhuzamosan feldolgozásokat futtató kognitív rendszerként sokkal több információ feldolgozására képes, mint a lassú és sorosan működő 2. típus. Az 1. típusú gondolkodás heurisztikus természetű, azaz tapasztalatokon alapuló közelítő becsléseket eredményez. Önmagában

⁹ KAHNEMAN, Daniel (2013): Gyors és lassú gondolkodás, HVG Könyvek, p. 28.

¹⁰ Például megyek az utcán, kávét iszom papírpohárból szívószállal, beszélgetek valakivel és közben a zöldnél átmegyek a zebrán. Ez a cselekvéssor több egyidejű gondolkodási szálát feltételez.

az, hogy jelenleg itt vagyunk elég meggyőző bizonyítéka annak, hogy evolúciós fejlődésünk során ez a típusú gondolkodás elégséges volt túlélésünkhöz.

Mindezekkel együtt a 2. típusú gondolkodás egyik kritikus feladata, hogy időről időre *felülírja* az 1. típusú gondolkodást. Erre azért van szükség mert noha az 1. típusú gondolkodás gyors és közelítőleges pontosságú eredményei a legtöbb helyzetben kielégítő megoldásnak bizonyulnak, sok esetben ezek az eredmények pontatlanok, félrevezetőek, bizonyos esetekben pedig teljesen tévesek lehetnek. Igen lényeges szempont az is, hogy az 1. típusú gondolkodás hatékonysága kognitív szempontból „jóindulatú” környezetet feltételez. Kognitív szempontból „ellenséges” környezetben – ahogy az később bemutatásra kerül – az 1. típusú gondolkodásra történő hagyatkozás komoly hibákhoz vezethet.

Az 1. típusú gondolkodás felülírása a 2. típusú gondolkodással azonban korántsem egyszerű. Az emberek általában kognitív szempontból is *spórolósak*, azaz, öntudatlanul is igyekeznek a lehető legkisebb energiát fordítani a szükséges mentális feldolgozáshoz, márpedig ennek a feltételnek a leegyszerűsítő, hozzávetőleges eredményeket szállító, de gyors 1. típusú gondolkodás maradéktalanul megfelel. A spórolás jelenségének megint csak evolúciós háttere van, igyekszünk minden feladatot a lehető legkisebb erőfeszítéssel megoldani, így tartalékolva kapacitást az esetlegesen felmerülő további problémák kezelésére. Ennek megfelelően öntudatlanul is hajlamosak vagyunk leegyszerűsíteni az előttünk álló konkrét problémát egy olyan problémára amely már ismerősnek, s így könnyen megoldhatónak tűnik¹¹, még akkor is, ha az így kapott megoldás jelentősen gyengébb, mint ami előállna az eredeti probléma tüzesebb vizsgálatával.

Kognitív torzításaink döntő többsége pontosan abból fakad, hogy a 2. típusú kifinomultabb, analitikus gondolkodásunk nem képes felülírni az alapértelmezett 1. típusú heurisztikus gondolkodást azokban az esetekben, amikor erre a helyzet összetettségéből fakadóan szükség lenne. A kognitív torzítások másik oka, hogy bizonyos esetekben ugyan sikerül a felülírás, de nem áll rendelkezésre az a *mindware*, azaz a tudás, amellyel a probléma sikeresen megoldható lenne.

2.3. Példák kognitív torzításra

2.3.1. Téves szillogizmus

A szillogizmus olyan következtetést jelent, melyben egy kijelentés (a konklúzió vagy következmény) két másik, igaznak feltételezett kijelentésből (a premisszákból vagy feltételekből) feltétlenül következik:

„Minden ember halandó” és „Én ember vagyok” (premisszák)
amelyekből következik, hogy
„Én halandó vagyok” (konklúzió)

¹¹ Attribute substitution

Most tekintsük a következő szillogizmust:

„Minden görög ember harcos” és „Szókratész harcos” (premisszák)

amelyekből következik, hogy

„Szókratész görög ember” (konklúzió)

Többségünknek elsöre nem tűnik fel, hogy ez a szillogizmus hibás és a konklúzió (bár önmagában igaz, de) téves következtetésen alapul. A példa emlékeztet egy helyes szillogizmusra és alapértelmezett 1. típusú gondolkodásunk e hasonlóság alapján gyorsan feldolgozza a rendelkezésre álló információt anélkül, hogy észrevenné az alaposabb vizsgálat (2. típusú gondolkodás) nyomán előtűnő nyilvánvaló hibát. Ugyanezt a példát helyettesítsük be egy más névvel:

„Minden görög ember harcos” és „Napóleon harcos” (premisszák)

amelyekből következik, hogy

„Napóleon görög ember” (konklúzió)

Ebben a második esetben nehézség nélkül képesek vagyunk felülírni az 1. típusú gondolkodást, hiszen Napóleon egy ismert történelmi személy, akiről pontosan tudjuk, hogy nem görög. Mindazonáltal a példa jól mutatja, hogy milyen könnyedén lehet téves következtetésre jutni a heurisztikus 1. típusú gondolkodás felülírása nélkül.

2.3.2. Összekötési torzítás

Egyes esetekben a felülírási nehézség kiegészül a mindware elégtelenségével és e két faktor együttesen okoz nehézséget a helyes válasz megadásában. Tekintsük a következő kérdést:

János 34 éves, intelligens de elég szűk látókörű férfi, akinek megrögzött szokásai vannak és általában meglehetősen halvérű. Az iskolában kitűnően teljesített matematikából, de a humán tárgyak, művészetek egyáltalán nem érdekelték.

Az alábbi két kijelentésben megfogalmazottak közül melyik a valószínűbb?

- 1. János könyvelő és gitáros egy rock-zenekarban.*
- 2. János gitáros egy rock-zenekarban.*

A megkérdezettek óriási többsége az 1. kijelentésben megfogalmazottat jelöli meg helyesként¹², miközben a helyes válasz a 2. Ez azért van így, mert két esemény együttes bekövetkeztének valószínűsége soha nem lehet nagyobb, mint bármelyik esemény egyedüli bekövetkeztének valószínűsége.

¹² Saját, publikálás előtt álló tanulmányban bemutatott kísérletben a válaszadók 10.53%-a oldotta meg helyesen a feladatot. MAKAY, Máttyás (2017): Cognitive Debiasing In College Environment (publikálás előtt)

$$p(A) \geq p(A+B)$$

aminek megfelelően,

$$p(\text{gitáros egy rock-zenekarban}) \geq p(\text{gitáros egy rock-zenekarban} + \text{könyvelő})$$

Azaz, annak a valószínűsége, hogy János gitáros egy rock-zenekarban mindenképpen nagyobb, mint annak a valószínűsége, hogy János gitáros egy rock-zenekarban és ugyanakkor könyvelő is¹³.

A hibás válaszok oka, hogy a legtöbb válaszadónál az 1. típusú alapértelmezett gondolkodás dolgozza fel a rendelkezésre álló információkat. János bemutatásából olyan benyomás alakul ki, amely sokkal inkább egy könyvelő felé mutat, semmint egy rockzenész felé. Ahhoz, hogy helyes válasz születhessen, ezt a gyors benyomást felül kell írunk, ráadásul fel kell ismernünk hogy a kérdés matematikailag is megfogalmazható és csak ezután, a 2. típusú analitikus gondolkodás segítségével érkezhünk el a matematikailag helyes de az eredeti intuíciónknak ellentmondani látszó eredményhez.

2.3.3. Prevalencia¹⁴ torzítás

Egészségügyi statisztikákból tudjuk, hogy 50 év fölött a nők 1%-a betegszik meg emlőrákban. A mammográfia 80%-os pontossággal mutatja ki a betegséget (a betegségben szenvedő és a tesztet elvégző nők 80%-ánál jelzi a betegséget, a maradék 20%-ban azonban sajnos nem), viszont 9%-ban fals pozitív eredményt ad, tehát kimutatja a betegséget, miközben az nincs jelen a páciensben. Ildikó már elmúlt 50 éves, letesztelt az orvos és a teszt pozitív eredménnyel zárul. Mekkora a valószínűsége, hogy Ildikó emlődaganatban szenved?

A legtöbb válaszadónak nehezebbé esik akár csak nagyságrendileg is meghatározni a helyes választ. Néhányan „intuíciora” alapozva tippelnek, de csaknem minden esetben meglehetősen távol járnak a helyes eredménytől¹⁵. Ebben az esetben a probléma első benyomásra is bonyolult, így a legtöbb embernek nem esik nehezebbé átkapcsolni a 2. típusú gondolkodásra. Csakhogy ez a jelen esetben nem elég, mert a helyes megoldáshoz valószínűségszámítási ismeretekre, vagy az ilyen típusú problémák strukturális ismeretére, azaz speciális mindware-re is szükség van.

¹³ A két valószínűség abban az esetben egyezhet meg, ha eleve kizárhatjuk az, hogy János könyvelő, de erre az eredeti információk birtokában nincsen módunk.

¹⁴ Prevalencia – Az adott időpontban, ill. időszakban egy adott populációt érintő jelleg (pl. betegség) előfordulási gyakorisága.

¹⁵ Ez egy feltételes valószínűségi probléma, amely többféle módon is megoldható (pl. Bayes képlettel), de a pontos metodológia nélkül is lehetséges körültekintő becslést adni a helyes értékre, ami 8.24% (nyolc-egész huszonnégy-század százalék). Saját, publikálás előtt álló tanulmányban bemutatott kísérletben a válaszadók mindössze 15%-a adott helyes becslést a kérdésre, míg a válaszadók csaknem fele nagyságrendileg is tévedett a válasz megadásánál. MAKAY (2017).

2.3.4. További példák kognitív torzításokra

A téves szillogizmus, az összekötési torzítás és a különböző valószínűségi torzítások mellett sok tucat egyéb, különböző gyökerű kognitív torzítás létezik. Ezek közül néhány ismertebb:

Megerősítési torzítás – Az a tendencia, hogy az emberek azokat az információkat részesítik előnyben, amelyek igazolják saját előfeltételezéseiket vagy hipotézisüket, miközben az ezen előfeltételezéseiket nem alátámasztó információkat hajlamosak figyelmen kívül hagyni.

Lehorgonyzási torzítás – Az a tendencia, hogy az emberek az elsőként megismert információt veszik aránytalanul a legnagyobb súllyal figyelembe egy adott probléma vizsgálatánál.

Visszamenőleges bölcsesség – Az a tendencia, hogy az emberek a végkifejlet ismeretében visszatekintve ezt a megvalósult eredményt evidensnek és előre láthatónak tekintik, miközben a történetek előtt objektíven szemlélve a legkevésbé sem volt biztos, hogy ez a végkifejlet fog bekövetkezni.

Szerencsejátékosok tévedése – Az a feltételezés, hogy ha egy esemény egy adott időszak alatt gyakrabban történik a szokásosnál (pl. ötször egymás után a piros jön ki a ruletten), akkor a következő időszakban, ezt „kiegyenlítő”, majd ritkábban fog történni (ezután már „biztosan” fekete jön).

Status Quo torzítás – Az a tendencia, hogy az emberek megítélésében a mindenkori jelenlegi helyzet, aránytalan előnyt élvez a döntéshozatal során, minden ettől való eltérés veszteségként értelmeződik.

Hozzáférhetőségi torzítás – Az a tendencia, hogy a könnyen hozzáférhető információ konkrét jelentőségéhez képest aránytalanul nagy súllyal esik latba egy helyzet megítélésénél, egyszerűen azért, mert különösebb erőfeszítés nélkül hozzá lehet jutni.

Torzítási vakfolt – Az a tendencia, hogy az emberek viszonylag könnyen felismerik más emberek kognitív torzításait, miközben a sajátjaik létezése rejtve marad előttük.

2.4. Miért döntő fontosságú a kognitív torzítások ismerete?

A kognitív torzítások drasztikusan képesek csökkenteni gondolkodásunk hatékonyságát. A magas intelligencia és tájékozottság általánosan nagyra értékelt szellemi tulajdonságok, de ha kognitív folyamataink hibás mintázatokat mutatnak, akkor mindezen képességek megléte mellett is gondolkodásunk végeredménye elkerülhetetlenül téves lesz.

A kognitív torzítások szisztematikusan eltérítik gondolkodásunkat az ismeretelméleti szempontból vett racionalitástól, ezzel csökkentik problémamegoldó

erejét és hatékonyságát. Ennek a mozzanatnak a jelentősége tovább sokszorozódik, ha a munka világának bizonyos szegmenseit tekintjük. Némely iparágak magas kockázatokkal, nagy bizonytalanságokkal, nagy nyomással jellemezhető, gyorsan változó vagy érzékeny környezetben működnek, esetleg rendkívül sok, vagy éppen túl kevés megbízható információt nyújtó környezetben kell messzire kiható, nagy súlyú döntéseket meghozni. Ilyen szakmák az állami szférában többek között a titkosszolgálati, katonai, rendvédelmi és állami elemző-, valamint döntéselőkészítési területek, energetikai és alapvető infrastruktúrát működtető nagyvállalatok, egészségügyi intézmények stb. A magánszférában a pénzintézetek, biztosítók, energiacégek és minden olyan vállalat, ahol nagy és összetett, ipari, infrastrukturális, környezetvédelmi stb. projektekkel foglalkoznak. Ezen cégek operatív vezetésének döntései nemcsak magát a céget és szűkebb piacát érintik, hanem sokszor komoly és hosszútávú nemzetbiztonsági, gazdasági, szociális, környezetvédelmi stb. hatást gyakorolnak az intézmény tágabb társadalmi környezetére is. Ezeken a területeken a vázolt hatások figyelembevételével nem lehet eléggé hangsúlyozni a racionális gondolkodás követelményét.

2.5. Jóindulatú és ellenséges kognitív környezet

Egy másik igen lényeges megjegyzés, amit a heurisztikus (1. típusú) gondolkodással kapcsolatban meg kell jegyeznünk – és amire a cikk elején már történt utalás – az, hogy kognitív szempontból környezetünk korántsem jellemezhető jóindulatúnak¹⁶. Ez két okra vezethető vissza.

A modern nyugati társadalomban élő ember rendelkezésére álló információ mennyisége és összetettsége nem mérhető össze azzal a mennyiséggel és komplexitással, amely agyunknak és kognitív képességeink rendkívül hosszú evolúciós fejlődése során környezetünket jellemezte. Ma összehasonlíthatatlanul több¹⁷ és bonyolultabb¹⁸ feldolgozást igénylő információ között élünk, mint amire az evolúció kognitív folyamatainkat felkészítette. A biológiai evolúció sokkal lassabb folyamat, mint a társadalmi evolúció, így agyunk a társadalmi evolúció mentén létrejött igen bonyolult helyzetek feldolgozásában sok alkalommal hibázik.

A másik ok, hogy társadalmi környezetünk kognitív értelemben a legkevésbé sem mondható „jóindulatúnak”. Jóindulatúnak akkor nevezhetünk egy környezetet, ha az (a) hasznos támpontokat ad 1. típusú heurisztikus gondolkodásunk számára, illetve (b) nincsenek olyan személyek, akik saját megtévesztő viselkedésüket pont ezen heurisztikák kihasználására alakítják ki. A modern társadalomban számos erő

¹⁶ STANOVICH, Keith E – WEST, Richard F – TOPLAK, Maggie E (2016): The Rationality Quotient (RQ): Toward a Test of Rational Thinking, MIT Press, p. 321.

¹⁷ Egy 2008-as kutatás szerint egy amerikai naponta 105,000 szó információval találkozik, amelyet, ha kiegészítünk az álló- és mozgóképekkel, akkor naponta átlagosan 34 GB információt jelent. Bővebben: <https://www.tech21century.com/the-human-brain-is-loaded-daily-with-34-gb-of-information/> (Letöltés ideje: 2016. 12. 01.)

¹⁸ Ebből eredeztethető az a közismert jelenség például, hogy az emberek általában igen gyengék valószínűségek becslésében. 1. típusú gondolkodásunk evolúciója folyamán a legeslegutóbbi időkig nem találkozott olyan bonyolult társadalmi szituációkkal, ahol ennek a képességnek lényeges hozzáadéka lett volna. Bővebben: <https://www.scientificamerican.com/article/why-our-brains-do-not-intuitively-grasp-probabilities/> (Letöltés ideje: 2016. 12. 01.)

dolgozik azon, hogy kognitív torzításainkat kihasználva valamilyen előnyhöz jusson. Példának okáért az egész modern marketing iparág – legyen az kereskedelmi vagy politikai – alapvetően arra alapozza módszereit, hogy az embereknek általában gondot okoz a bonyolultabb információk racionális feldolgozása. Nincs okunk azt állítani, hogy ezek az erők eredendően rosszindulatúak lennének, de világosan kell látni, hogy a hozzánk eljutó információ manipulálásával ellenérdekeltek abban, hogy racionális döntéseket hozzunk.

3. A RACIONALITÁS KVANTITATÍV MÉRÉSE

Ahogy a cikk elején szó volt róla, ellentétben az intelligencia mérésével, amely komoly hagyományokat és széleskörű szakmai konszenzust, valamint társadalmi beágyazottságot mondhat magáénak, a racionalitás, mint kognitív képesség kvantitatív mérésének tudományos programja csak az utóbbi időkben gyorsult fel. E munka egyértelműen abban az irányban fejlődik, hogy lehetségessé váljon az IQ mintájára az RQ (Rationality Quotient – racionalitás hányados) megalkotása és mérési metodológiájának kialakítása. Ahogy az IQ, az adott illető intelligenciájának a viszonyító száma adna tájékoztatást az illető intelligenciájáról, az RQ, mint a racionalitás viszonyító száma tájékoztatna az illető racionális-gondolkodás képességéről. Hasonlóképpen, ahogy az IQ mértékének megállapítása speciális IQ teszttel történik, úgy az RQ meghatározása is speciálisan erre fejlesztett tesztekkel válik lehetségessé.

A Keith Stanovich által vezetett kutatócsoport egy hároméves kutatási program eredményeképpen létrehozta az RQ-teszt működő prototípusát, ami jó eséllyel lesz kiindulópontja minden további, ezen a területen végzett erőfeszítésnek.

3.1. Az RQ-teszt felépítése

A kutatócsoport által kidolgozott RQ teszt nagyjából két tucat altesztből épül fel, amelyek négy alapvető csoportba oszthatóak:

3.1.1. Az információfeldolgozás problémáira rámutató feladatok

Az ebbe a kategóriába tartozó tesztek azt mérik, hogy a válaszadók analitikus 2. típusú gondolkodása képes-e adott esetben felülírni az alapértelmezett heurisztikus 1. típusú gondolkodást (intuíció felülírása, hibás szillogizmusok, arányosság/abszolút érték tesztek), illetve – ami ugyancsak rendkívül lényeges – hogy ezt a felülírást képes-e a válaszadó a probléma megoldásához szükséges ideig fenntartani (szisztematikus érvelés teszt).

Ide tartoznak azok a tesztek is, amelyek azt mérik, hogy az alanyok mennyire képesek a lényeges és lényegtelen információk megkülönböztetésére (keretezés, lehorgonyzás és preferencia anomáliák teszt), valamint azok a tesztek amelyek a saját meglévő nézetrendszer torzító hatását mérik a racionális érvelés feldolgozásában (érvelések erősségének értékelése teszt). Végül, ebbe a kategóriába tartozik a saját kognitív képességek esetleges túlértékelését megmutató teszt is.

3.1.2. A hiányzó mindware-re rámutató feladatok

Ebbe a csoportba tartoznak azok a feladatok, amelyek megoldásához a felülíráson kívül általában egyéb mindware-re is szükség van (valószínűségi és statisztikai érvelés, tudományos érvelés teszt), illetve azok, amelyek összetettebb, de a mindennapi életben gyakran előforduló valószínűségi események helyes értelmezésének képességét mérik (valószínűség-számítási készség teszt).

Ebben a csoportban kapott helyet a pénzügyi és közgazdasági ismereteket és logikát mérő teszt, a szintén elemi valószínűség-számítási képességeket mérő várható érték teszt, illetve a valóságos életben felmerülő kockázatok valódi mértékének felismerését mérő teszt is.

3.1.3. Fertőzött mindware meglétére utaló feladatok

A „fertőzött mindware” azokra a saját hitekre és nézetekre utal, amelyek megnehezítik a beérkező információk racionális feldolgozását. Ezek nem konkrét kognitív torzítások, inkább olyan gondolkodási mintázatok, amelyek tartósan akadályozzák a racionális gondolkodást. Ebbe a csoportba tartoznak a babonás és a tudományellenes gondolkodást mérő tesztek, az összeküvéseleméletekre való fogékonyságot mérő teszt, illetve a működésképtelen saját hitek meglétét megmutató teszt.

3.1.4. Racionális információ-feldolgozást elősegítő gondolkodási diszpozíciókat mérő skálák

Az ebbe a csoportba tartozó kérdéssorok olyan általános gondolkodási diszpozíciókat mérnek, amelyek lényeges háttérrel biztosítanak a racionális gondolkodáshoz. A csoport több szempontból is különbözik az első háromtól.

Az első három csoportba tartozó tesztek értékelése egyszerű skálán történik. Ha mondjuk 6 kérdés foglalkozik a keretezési torzítással, akkor 6 pont jár azért, ha az összes feladatot helyesen oldja meg a válaszadó, tehát nem mutatható ki nála a keretezési torzítás. A racionális gondolkodás képességének vizsgálata szempontjából nyilván ez az maximálisan jó eredmény. A gondolkodási diszpozíciók értelmezése ennél összetettebb, ezeknél nem a maximum értéket keressük, hanem valamiféle optimumot. Ezen diszpozíciók szélsőértékei általában nem kedveznek a racionális gondolkodásnak, de ezen túl önmagában a teszten mért eredmények nem értelmezhetők olyan egyértelműen, mint az első három csoportba tartozó skálák. A négy vizsgált gondolkodási diszpozíció értékei így nem is számítanak be a konkrét teszteredménybe, hanem a kvantitatív eredmény mellé adnak egyfajta – igen hasznos – háttérrel¹⁹.

¹⁹ Ezek a diszpozíciók természetesen tovább bonthatók további gondolkodási jellemzőkre. Az aktívan nyitott gondolkodás diszpozíció például magában foglalja az (1) episztemológia abszolutizmus kerülésének képességét, a (2) perspektíva-váltás képességét, a (3) dekontextualizálás képességét, valamint az (4) alternatív vélemények és bizonyítékok megfontolásának képességét. STANOVICH et al. (2016) p. 209.

Feldolgozási problémákra rámutató feladatok	Hiányzó mindware-re rámutató feladatok	Fertőzött mindware meglétére utaló feladatok	Racionális információ-feldolgozást elősegítő gondolkodási diszpozíciókat mérő skálák
- Valószínűségi és statisztikai érvelés teszt - Tudományos érvelés teszt		- Babonás gondolkodás teszt - Tudomány-ellenes gondolkodás teszt	- Aktívan nyitott gondolkodás teszt - Deliberatív gondolkodás teszt
- Spórolós információ-feldolgozásra utaló tesztek - Intuíció felülírása teszt - Hibás szillogizmusok teszt - Arányosság és abszolút érték teszt - Szisztematikus érvelés teszt	Valószínűség-számítási készség teszt	Összeesküvés-elméletek teszt	Jövő-orientált gondolkodás teszt
- Lényegtelen információk figyelembevételére utaló tesztek - Keretezés teszt - Horgonyzási torzítás teszt - Preferencia animáliák teszt	Pénzügyi és közgazdasági logika teszt	Működésképtelen személyes hitek teszt	Érzelmek tudatosításának képessége teszt
- Saját nézetrendszer túlértékelésére utaló tesztek - Érvelések erősségének értékelése teszt	Várható érték helyes felismerése teszt		
- Túlzott magabiztosságra utaló tesztek - Saját ismeretek reális értékelése teszt	Kockázatok ismerete teszt		
Időbeli diszkontálás teszt			

2. ábra²⁰

²⁰ STANOVICH et al. (2016) p. 64.

3.2. Az RQ-teszt gyakorlati összeállítása

A könyv természetesen nem tartalmazza a tesztben szereplő többszáz kérdést, de az elméleti alapok részletes tárgyalásával és a struktúrára vonatkozó pontos információkkal lehetővé teszi a kérdőív rekonstrukcióját.

3.2.1. Feladatok és súlyozás

A magyar változat végül 365 kérdést tartalmaz, ez valamivel kevesebb, mint az eredeti változat, de a lényegi arányokat ez nem érinti. Némely fejezeteknél (pl. közgazdasági és pénzügyi logika, összeesküvés elméletek) – az eltérő kulturális környezet miatt – a kérdések eltérnek az eredetitől, de ez a mérésben nem okoz gondot. A 365 kérdésből 317 pontozott kérdés, míg 48 kérdés vonatkozik a gondolkodási diszpozíciókra, ezek, ahogy jeleztük, nem számítanak bele az RQ értékebe, mindazonáltal nagyon hasznos háttér-információval szolgálnak. A mért kérdésekre összesen 150 pontot lehet szerezni, ebben a tesztben ez az RQ maximális értéke. Az egyes feladatsorok súlyozását a saját szerkesztésű **3. ábra mutatja**, amely a következőképpen alakult:

	<i>CART fejezetek</i>	<i>Feladatszám</i>	<i>Pontszám</i>
1.	Valószínűségi és statisztikai érvelés	18	18
2.	Tudományos érvelés	23	20
3.	Intuíció felülírása	10	10
4.	Híten alapuló elfogultság a szillogisztikus érvelésben	16	8
5.	Abszolút érték figyelembevétele arányosság helyett	6	6
6.	Szisztematikus érvelés	5	5
7.	Keretezési torzítás	6	6
8.	Horgonyzási hatás	8	4
9.	Preferencia anomáliák	5	5
10.	Az érvelés értékelése teszt	15	5
11.	Saját ismeretek reális értékelése	51	6
12.	Racionális időbeli diszkontálás	15	7
13.	Valószínűségszámítási készség	9	9
14.	Pénzügyi és közgazdasági racionalitás	24	8
15.	A várható érték helyes felismerése	10	5
16.	Kockázatok ismerete	10	3
17.	Babonás gondolkodás	12	5
18.	Tudományellenes gondolkodás	12	5
19.	Összeesküvés elméletek	20	10
20.	Működésképtelen saját hitek	9	5
(21.)	Gondolkodási diszpozíciók (aktívan nyitott gondolkodás, deliberatív gondolkodás, jövőorientáció és érzelmek azonosításának képessége)	48	-
	ÖSSZESEN	365	150

3.2.2. A kérdések sorrendje és formája

A kérdések végső sorrendje bonyolult szabályok szerint alakult ki. Bizonyos kérdéscsoportok (pl. valószínűségi és statisztikai érvelés, kockázatok ismerete) kérdései szimplán egymás után következnek, míg más fejezetek kérdései (pl. keretezés, horgonyzás) a tesztben egymástól távol, szórta helyezkednek el, mert ezekben az esetekben lényeges szempont, hogy a válaszadó számára ne legyen evidens, hogy melyik kérdés mit és milyen módon mér.

A kérdések változatos formában jelennek meg. Egy részük (pl. intuíció felülírása), hasonlóan például egy intelligencia teszthez, világosan belátható – általában többválasztós – feladat formájában jelenik meg. A kérdések egy másik részének célja homályban marad (pl. keretezés, horgonyzás), míg egy harmadik részének (pl. saját ismeretek reális értékelése, érvelések erejének értékelése) célja általában – a teszt célja érdekében szándékosan – teljesen megtéveszti a válaszadókat.

A teszt viszonylag hosszú. Ügyeltünk arra, hogy a teszt elején legyenek a nagyobb fókuszálást kívánó, „nehezebb” kérdések, míg a tesztalanyok valószínűsíthető fáradásával párhuzamosan, a vége felé legyenek az egyszerűbben megválaszolható, önbevallásra épülő kérdések.

3.2.3. Technológia és kiértékelés

A teszt elvileg papír alapon is kitölthető, de gyakorlatban vélhetően csaknem kizárólag elektronikusan fog történni. A kérdőív hosszúsága, a számos együtt értékelendő, de egymástól távol lévő kérdés (pl. keretezési kérdések), illetve néhány kérdéscsoport bonyolult statisztikai számításokat igénylő kiértékelési módszere (pl. érvelés erősségének értékelése kérdéscsoport²¹) a kiértékelést csaknem bizonyosan számítógéphez köti.

A magyar változat kérdőív részét Google Forms-ban készítettük el, míg a kiértékelést az előre felparaméterezett Google Sheets táblázatkezelő végzi. A teszt lebonyolítása egyszerű, a tesztalany egy számítógépen a Google Forms letisztult felületén egyenként megválaszolja a kérdéseket, majd a teszt-vezető a Google Forms-ból egyszerűen átemeli az adatokat a Google Sheets előzetesen elkészített táblázatába, ahol pár tizedmásodperc múlva rendelkezésre állnak a nyers és összesített kiértékelési adatok.

3.3. Kritikai észrevételek

A felsorolt kritikai észrevételek tartalmazzák az amerikai kutatócsoport megjegyzéseit, illetve a saját, igen kevés és messze nem reprezentatív mintával elvégzett kísérleteink során felmerült szempontokat is.

3.3.1. Prototípus jelleg

²¹ Ebben a kérdéscsoportban a kiértékelés többváltozós regresszió módszerével történik, amelynek kézi kiszámolgatása a gyakorlatban csaknem kivitelezhetetlen.

A teszt jelen pillanatban magán hordozza a működő, de kevésbé kipróbált megoldások jellegzetességeit. Jelen pillanatban a teszt alkalmas arra, hogy rámutasson az egyes kitöltők kognitív torzításaira és arra is, hogy mért különbségeket mutasson ki több kitöltő képességei között. Mindazonáltal, miután jelenleg nem létezik széles körben elfogadott definíciója, skálája, metodológiája az RQ-nak, nem sokat tudunk mondani az RQ „átlagos” értékéről, szórásáról, stb. Mindezekhez az RQ koncepciójának széles körben történő elfogadására és évek tapasztalatára lesz szükség.

A korlátozott tapasztalat alapján viszonylag keveset tudunk minden teszt két kritikus jellemzőjéről, a pszichometriai értelemben vett *megbízhatóságáról* és *érvényességéről*. Az RQ teszt megbízhatósága érdekes kérdés. Egyfelől, miután a teszt döntő részében képességeket mér, azt várjuk, hogy – az IQ-teszthez hasonlóan – magas lesz a megbízhatósága. Másfelől, – ellentétben az IQ-val, ahogy erről később szó lesz – az RQ megfelelő tréninggel igen komoly mértékben növelhető, tehát a teszt (illetve annak altesztjei) kifejezetten alkalmasak arra, hogy az RQ változását is nyomon kövessék.

Az érvényességgel kapcsolatban is a használat elterjedésével fogunk pontosabb empirikus képet kapni. Mindazonáltal, igen meggyőző példák mutatják meg, hogy a közvetlenül való életből vett szituációk ismeretelméleti szempontból milyen kognitív torzítási csapdákat kínálnak fel²². Ezek a példák erősen alátámasztják azt a kiinduló feltételezést, hogy a racionalitás az intelligenciához mérhető fontosságú kognitív képesség, amelynek a mindennapi életben is komoly kihatásai vannak.

3.3.2. A teszt terjedelme

A teljes teszt hosszú, kitöltése legkevesebb 2-2 és fél órába telik, ami nem minden szituációban kivitelezhető, vagy kívánatos. A kutatócsoport megadja egy rövidített teszt struktúráját is, ahol 20 alteszt helyett 11, illetve 4 gondolkodási prediszpozíció helyett csak 1 szerepel, sőt egy végletekig lerövidített verziót is, amely csak az első két altesztet (valószínűségi és statisztikai érvelés, illetve a tudományos érvelés) tartalmazza és 25-30 perc alatt kitölthető. A rövidítéssel nyilván sokkal gyorsabbá és kényelmesebbé válik a teszt, de cserébe fontos dimenziók vesznek el, még ha ennek a két fejezetnek a megoldási eredménye közepesen erős korrelációt mutatott is a teljes teszt kitöltésének eredményével. A tesztet kitöltő alanyok egyébként saját kísérletünkben is megemlézték a túlzottnak ítélt hosszúságot, csakúgy mint azon HR szakemberek egy része, akiknek megmutattuk a rendszert.

A hosszúság megítélésénél azonban más szempontokat is érdemes figyelembe venni. Mindenekelőtt, ez a teszt – jelen formájában – nem „lakossági” teszt, hanem egy professzionális felhasználásra készített kérdőív. A teszt, azokban a munkakörökben használható a legjobban, amelyek nagy komplexitással, nyomással és felelősséggel járnak, azaz olyan munkakörökben, ahol általában amúgy is sok körös, több lépcsőből álló kiválasztási procedúra folyik. Ezekben a felvételi folyamatokban a teszt hossza vélhetően nem elsődleges szempont.

²² STANOVICH et al. (2016) pp. 297-311.

3.3.3. A teszt felépítése

Jelenlegi állapotában a teszt igen széles területet fed le. A gyakorlati alkalmazásban, főleg megismételt tesztek esetében, ennél szűkebb területet lefedő tesztek is készülnek majd. Igen érdekes a másik oldalról történő közelítés is, amikor azt vizsgálják, hogy az egyes stratégiai területeken mely típusú kognitív torzítások a legveszedelmesebbek²³. Ezen kutatások alapján szektor-, vállalat-, vagy akár munkakör-specifikus tesztek is lehet készíteni, amelyek kifejezetten az adott specifikus igényekre vannak szabva.

4. AZ RQ-TESZT FELHASZNÁLÁSI TERÜLETEI

4.1. Az RQ-teszt a kiválasztási folyamatban

A munkaerő-kiválasztási folyamatban általában két típusú teszt használatos a személyiségtesztek és a képességfelmérő tesztek. A *személyiségtesztek*²⁴ a jelentkező jellemző karakter- vagy személyiségjegyeit próbálják meg feltérképezni és mérhető, empirikusan igazolható adatokra lefordítani. A személyiségtesztek igen népszerűek és széles körben használtak a munkaerőpiaci kiválasztásban. Sokan mélyen hisznek ezen tesztek eredményeiben és komoly súllyal szerepeltetik a kiválasztási folyamatban²⁵.

A képességfelmérő tesztek a jelentkező valamelyik képességéről közölnek számszerűsített adatokat. Ezek közé tartozik prominensen az IQ-teszt, a figyelem tesztek (pl. Pieron) vagy a különböző szövegértési tesztek. Az RQ-teszt egyértelműen ide, a képességfelmérő tesztek kategóriájába tartozik és egy olyan alapvető kognitív képességre ad pontos rálátást, amelyet az eddig létező tesztjeink nem mértek, s így lehetővé teszi a kognitív képességeknek jóval kiegyensúlyozottabb feltérképezését a kiválasztási folyamatban.

²³ YUDKOWSKY, Eliezer: Cognitive Biases Potentially Affecting Judgment of Global Risks, <https://intelligence.org/files/CognitiveBiases.pdf> (Letöltés ideje: 2016. 12. 01.)

²⁴ A legnépszerűbb személyiségtesztek közé tartozik a CPI – (California Psychological Inventory – Kalifornia pszichológiai eszköztár), a BFQ – (Big Five Questionnaire – Big Five személyiségmodell), az MBTI – (Myers-Briggs Type Indicator – Myers-Briggs típusindikátor) és a Captain-analízis.

²⁵ A személyiségtesztekkel kapcsolatban szkeptikusabb szakértők a számos kritikai észrevételel fogalmazzák meg. Ezen érvelések szerint a személyiségteszteknek nincs igazán széles körben elfogadott teoretikus megalapozottságuk, a különböző elméletek egymáshoz képest is igen különböző alapfeltételezéseken nyugszanak. Lényeges az is, hogy nem áll rendelkezésre olyan adat amely megerősítené, hogy a személyiségtesztek eredményeinek bármilyen mérhető korrelációja lenne a későbbi vezetői teljesítménnyel. Végezetül pedig módszerükben ezek a tesztek általában önértékelésen, önbevalláson alapulnak, amely - dacára a különböző technikáknak, amelyek ezt nehezíteni hivatottak - mégiscsak ki van téve a manipulált válaszoknak. Lásd: PAUL, Annie Murphy (2004): The Cult of Personality Testing, Free Press

4.2. Az RQ-teszt használata a meglévő munkaerő körében

Viszonylag ritkán fordul elő, hogy meglévő munkatársakkal IQ-tesztet (vagy valamilyen más képességfelmérő tesztet) töltenek ki. Az intelligencia mértéke fiatal felnőtt korra kialakul és tovább nem növelhető, az életkor előrehaladtával pedig – fiziológiai okok miatt – csökkenő tendenciát mutat. Ez a csökkenés megfelelő életmóddal jelentősen fékezhető, de a tapasztalat azt mutatja, hogy az intelligencia érdemi növelésére nincsen mód, tehát nincs sok szakmai indoka újabb és újabb tesztek kitöltésének.

Az RQ-teszttel nem ez a helyzet. A racionális gondolkodás képességének fejlődése más, jelentősen eltérő életkori mintázatokat mutathat, és ami a legfontosabb, potenciálisan igen komoly mértékben fejleszthető. E fejlesztési folyamat különböző szakaszaiban az RQ-teszt képes e fejlődést kvantitatív méréssel folyamatosan nyomon követni.

A racionális gondolkodás fejlesztésének legfontosabb módszere a kognitív torzítások csökkentése és ez ma az egyik legizgalmasabb terület a kognitív pszichológiában. Jelentős számú kutatási program, köztük komoly finanszírozású katonai programok²⁶ is működnek e területen. A kísérletek azt mutatják, hogy a kognitív torzítások erősen különböző környezetekben és igen változatos módszerekkel is hatékonyan csökkenthetők²⁷. Ezek az eredmények egyedülálló perspektívát nyitnak a munkaerő képzésében, mert egy olyan alapvető képesség számottevő növelése válik lehetővé, amely döntő módon lesz hatással a munkaerő teljesítményére.

ÖSSZEFOGLALÁS

A kognitív torzítások kvantitatív mérése egy dinamikusan fejlődő kutatási program. Csaknem bizonyosnak tűnik, hogy az RQ belátható időn belül – a hosszú idő óta, széles körben használt IQ kiegészítőjeként – a kognitív képességek egyik

²⁶ Az utóbbi idők egyik legérdekesebb kísérletét a kognitív torzítások területén a Leidos Inc. végezte el az Amerikai Egyesült Államok Légierője kutatási programján belül az Air Force Research Laboratory-val együttműködve. A kísérlet során a kiválasztott kognitív torzítások csökkentését egy erre a célra fejlesztett nagy költségvetésű videojátékon alapuló tréninggel végezték egyetemistákból és aktív katonai hírszerzőkből álló csoportok esetében. A kísérlet igen biztató rövid és hosszabb távú eredményeket mutatott, a torzításokat rövid távon 25%-kal (egyetemisták) és 27%-kal (hírszerzők), míg hosszabb távon 25% és 26%-kal sikerült csökkenteni. Lásd: MOREWEDGE, Carey K. – YOON, Haewon – SCOPELLITI, Irene – SYMBORSKI, Carl W – KORRIS, James H – KASSAM, Karim S (2015): Debiasing Decisions: Improved Decision Making With a Single Training Intervention és SYMBORSKI, Carl W – BARTON, Meg – QUINN, Mary – MOREWEDGE, Carey K. – KASSAM, Karim S. – KORRIS, James H (2014): Missing: A Serious Game for the Mitigation of Cognitive Biases

²⁷ Saját publikálás előtt álló kutatásunkban a kognitív torzítások csökkentésének lehetőségét egy tipikus egyetemi környezetben (nagy számú résztvevő, frontális tréning és korlátos időtartam) teszteltük. Rövid távon az összekötési torzítást 35%-kal, míg a prevalencia torzítást 33%-kal sikerült csökkentenünk és ennek a jelentős része hosszabb távon is megmaradt. MAKAY (2017)

meghatározó mérőeszközzé válik. A racionalitás mérése egy olyan alapvető kognitív képességre ad pontos rálátást, amelyet az eddig létező tesztheink nem mértek, így téve lehetővé a kognitív képességeknek jóval kiegyensúlyozottabb feltérképezését mind a kiválasztási folyamatban, mind a meglévő munkaerő értékelésénél.

A meglévő munkaerő körében végzett racionalitás-mérés kiváló kiinduló alapot és folyamatos kvantitatív értékelési lehetőséget biztosít a kognitív torzítások csökkentésére kialakított programok számára. Ezek a tréningek a racionális gondolkodás képességének javításával döntő mértékben járulhatnak hozzá a meglévő munkatársak kognitív képességeinek növeléséhez és ezen keresztül a szervezetben futó munkafolyamatok hatékonyságának javításához.

Felhasznált irodalom:

- FLANAGAN, Dawn, P – DIXON, Shauna G (2014): The Cattell-Horn-Carroll Theory of Cognitive Abilities, <http://onlinelibrary.wiley.com/store/10.1002/9781118660584.ese0431/asset/ese0431.pdf?v=1&t=iyskff0s&s=72ef0f84b9cff4a230f31feb5a69d59c9e114898> (Letöltés ideje: 2016. 12. 01.)
- KAHNEMAN, Daniel (2013): Gyors és lassú gondolkodás, HVG Könyvek
- MAKAY, Mátyás (2017): Cognitive Debiasing In College Environment (publikálás előtt)
- MOREWEDGE, Carey K. – YOON, Haewon – SCOPELLITI, Irene – SYMBORSKI, Carl W – KORRIS, James H – KASSAM, Karim S (2015): Debiasing Decisions: Improved Decision Making With a Single Training Intervention, https://www.researchgate.net/publication/281206303_Debiasing_Decisions_Improved_Decision_Making_With_a_Single_Training_Intervention (Letöltés ideje: 2016. 12. 01.)
- PAUL, Annie Murphy (2004): The Cult of Personality Testing, Free Press
- STANOVICH, Keith E (2009): What Intelligence Tests Miss: The Psychology of Rational Thought, Yale University Press
- STANOVICH, Keith E (2011): Rationality and the Reflective Mind, Oxford University Press
- STANOVICH, Keith E – WEST, Richard F – TOPLAK, Maggie E (2016): The Rationality Quotient (RQ): Toward a Test of Rational Thinking, MIT Press
- SYMBORSKI, Carl W – BARTON, Meg – QUINN, Mary – MOREWEDGE, Carey K. – KASSAM, Karim S. – KORRIS, James H (2014): Missing: A Serious Game for the Mitigation of Cognitive Biases, http://www.iitsec.org/about/PublicationsProceedings/Documents/BP_TRNG_14295_Paper.pdf (Letöltés ideje: 2016. 12. 01.)
- YUDKOWSKY, Eliezer: Cognitive Biases Potentially Affecting Judgment of Global Risks, <https://intelligence.org/files/CognitiveBiases.pdf> (Letöltés ideje: 2016. 12. 01.)

- Creative Technologies Inc., <https://cretecinc.com/portfolio/intelligence-advanced-research-projects-activity-iarpa-sirius-program/> (Letöltés ideje: 2016 12. 01.)
- Tech21century (<https://www.tech21century.com/the-human-brain-is-loaded-daily-with-34-gb-of-information/>) (Letöltés ideje: 2016 12. 01.)
- Scientific American <https://www.scientificamerican.com/article/why-our-brains-do-not-intuitively-grasp-probabilities/> (Letöltés ideje: 2016 12. 01.)

DR. DÁVID FERENC

**A BIZTONSÁG ÉS NEMZETBIZTONSÁG MEGISMERÉSÉNEK SZÁLA:
TUDOMÁNYOS-ISMERETTERJESZTŐ ELŐADÁSOK A „KUTATÓK
ÉJSZAKÁJÁN”**

Az egyetemeken, kutatóhelyeken, közintézményekben évről-évre, idén 12. alkalommal megrendezett „Kutatók éjszakája” nagy országos népszerűségnek örvend. A kezdeményezés az európai együttműködésnek és az Európai Unió Bizottságnak köszönheti létrejöttét; általános ismeretterjesztő célkitűzései mellett fontos szerepet játszik a kutatói és tudományos pálya népszerűsítésében, a fiatalabb hallgatóság megnyerésében, a kutatási eredmények minél szélesebb körű, mégis közérthető formában történő disszeminációjában. A Nemzeti Közszerződési Egyetem 2017. szeptember 29-én, pénteken, nyolc helyszínen 83 előadással és 6 ismétlődő bemutatóval, összesen 118 programra várta a majdnem 3200 fő érdeklődőt a kora délutántól késő estig tartó rendezvényén.



Az egyetemi programkínálat részeként három tematikus előadássorozatnak a Hungária körúti kampusz adott otthont. Ugyanitt került már negyedik alkalommal megrendezésre az egyetem Nemzetbiztonsági Intézetének önálló szekciója, ahol tíz változatos és érdekes előadásra ülhetett be a hallgatóság. Az előadók az intézet Katonai és Polgári Nemzetbiztonsági, valamint Terrorrelhárítási Tanszékének oktatói és kutatói állományából kerültek ki egy-egy általuk előzetesen megjelölt tudományos-ismeretterjesztő előadással. A tíz programelem a nemzeti és nemzetközi biztonság, a terrorrelhárítás, valamint a hadtörténelem és jogtudomány megannyi (rész)területét fogta át, kínálta a közönségnek.

Resperger István egyetemi docens, az intézet igazgatója több fegyveres konfliktust fűzött fel egy logikai láncre, hogy bemutassa a fegyveres küzdelem, mint a hadtudomány alapvető kutatási tárgyának összefüggésrendszerét. A fegyveres konfliktus elemzésének módszertana során megannyi elemmel számolt és igyekezett közös értelmezési felületet kínálni egy korszakokon átívelő, múlt és napjaink háborúit egységes értelmezési keretbe helyező elemzésével „Világok háborúja, a háborúk világa” című előadásában.¹ A háborúban kulcsfontosságú információs fölény szerepét Kaiser Ferenc egyetemi docens, az intézet tanszékvezetője egy,

¹ Kutatási területéhez lásd bővebben: Az aszimmetrikus hadviselésre adható válaszok. Honvédségi szemle 2017/1. pp. 24-43., vagy Aszimmetrikus hadviselés a modern korban. Zrínyi Kiadó, Budapest, 2013.

hadászati és harcászati kérdéseket is magába foglaló hadtörténeti előadással készült.² „*Hadászati és harcászati felderítés a Midway-szigetekenél vívott tengeri csatában*” cím alatt egy, a hallgatóság által ismert összecsapás köztörténeti megismerése mellett rávilágított az amerikai fél győzelmének alapjára. Előadásában amellet érvelt, hogy bár a japánok többszörös előnyben voltak az amerikai félle szemben, de az „információs fölény” meghatározó szerepet játszott utóbbiak győzelmében. Kiemelte, hogy az események sematikus, a tengeri hadműveletek ismertetésén felül különleges és meghatározó szerepe volt a résztvevők felderítésének és hírszerzésének. Regényi Kund adjunktus egy ismeretterjesztő előadást ötvözött egy fegyvertörténeti és technikai bemutatóval, amikor „*Az első világháború innovatív lövészetű fegyverei*” címmel nem csak két technikaitörténeti korszak között épített hidat, de rávilágított egy történeti korszak állásháborúinak harci és harcászati sajátosságaira, a megváltozott körülmények által katalizált technikai fejlődésre, ami hatásait még évtizedekkel később is éreztette.³ Szabó Károly egyetemi tanársegéd, egy napjainkban ismert társadalmi-lélektani kérdés fontosságát emelti ki és hangsúlyozta a hallgatóságnak. „*Nemzetbiztonsági percepció, avagy féljünk együtt*” című előadásában társadalmi-politikai közegében ábrázolta az egyént, a közösség tagjait, aki(k) térben és időben, az őket érő környezeti ingerek hatására alakítják ki saját biztonsági percepciójukat, ami – természetéből adódóan – legalább annyira lehet objektív és szubjektív, mint irányított és befolyásolható.⁴ Dely Péter az egyetem doktorandusza kutatási témájának egy szeletét, „*Szürke műveltek Afganisztánban – kábítószerbűnözés*” címmel tartott előadásában mutatta be.⁵ A prezentáció ismertette a nemzetközi közösség afganisztáni szerepét és fejlesztési törekvéseit egy véget nem érő, a kábítószertermesztés problémájával nap mint nap találkozó küzdelmet, ami még mindig csak az út egy szakasza a feltételezett és várva-várt polgári életbe történő békés átmenetnek.

A programsorozatban külön részt képeztek a terrorelhárítással foglalkozó tematikus előadások. Jasenszky Nándor szakoktató „*A terrorizmus és terrorelhárítás evolúciója*” című előadásában a terrorizmus és vele szembeni fellépés történelmi szálát fűzte össze, miközben a fejlődési ívet egészen napjainkig vezette le a hallgatóság aktív közreműködése mellett.⁶ Őt követte Kasznár Attila egyetemi adjunktus, az intézet tanszékvezetője, aki „*Terrorizmus a globális térben*” cím alatt napjainkban gyakran idézett kérdésekre kereste a választ. Előadásában az elmúlt évek európai terrortámadásait hozta fel példaként és nemzetközi trendeket mutatott be, miközben értelmezési keretet kínált a biztonsági helyzet és terrorizmus

² Történeti és tengeri hadelméleti kutatásaihoz lásd: Az Amerikai Egyesült Államok haditengerésze. *Nemzet és biztonság* 2009/9. pp. 40-54., ill. A blokádmélete és gyakorlata a tengeri hadviselésben. *Aetas* 2007/4. pp. 49-68.

³ Kutatásaihoz lásd: Szakmatörténeti szemelvények. Nemzetbiztonsági Szakszolgálat, Budapest, 2014. vagy Hírszerzési és Kémelhárítási Szabályzat a két világháború között. *Nemzetbiztonsági Szemle* 2015/3. pp. 155-197.

⁴ Bővebben: Gondolatok a katonai elhárításról. *Szakmai szemle* 2015/1. 7-15., illetve A katonai elhárítás és a műveleti biztonság. *Szakmai szemle* 2016/1. pp. 108-119.

⁵ Kutatásairól lásd: Kábítószer és kábítószer-bűnözés Afganisztánban. *Belügyi szemle* 2016/3. pp. 5-15., illetve Afganisztán Nemzeti Rendőrsége I. *Nemzetbiztonsági Szemle* 2015/2. pp. 37-51.

⁶ Lásd még: A terrorelhárítás információéhsége és a „csillapítás” lehetőségei. és Nagy kockázatú akciók, avagy a terrorelhárítók mindennapjai. In: Bebesi Zoltán (szerk.): *Terrorelhárítási alapismeretek*. Dialóg Campus Kiadó, Budapest, 2016. pp. 193-212. és 263-296.

kapcsolatának megértéséhez.⁷ Előadásához csatlakozott Hankiss Ágnes címzetes egyetemi docens, aki „*Magányos farkasok vagy terrorista hálózatok? A terrorizmus új jelenségei*” című előadásában az egyén és terrorcselekmény kapcsolatát, az úgynevezett „magányos farkas” elkövetők jelenségét vizsgálta és helyezte el egy, a magányos egyénnél lényegesen szélesebb rendszerben.⁸ Bács Zoltán György szakoktató a terrorizmus és turizmus fogalompárt húzta közel egymáshoz, amikor „*Turizmus a terrorizmus árnyékában*” címmel biztonsági szempontokkal és az elővigyázatosság nélkülözhetetlenségével kötötte össze a turisztikai gondolkodást.⁹

Összegezve megállapítható, hogy az egyetem Nemzetbiztonsági Intézete a 2017. évben is sikeresen vett részt a „Kutatók éjszakáján”; az elmúlt évekhez hasonlóan több előadással, önálló szekcióval és népes hallgatóság előtt állt helyt a rendezvény célkitűzéseiben foglalt tudományos-ismeretterjesztő tevékenység megvalósításában.

⁷ Kutatásaihoz lásd még: A terrorizmus megjelenése Magyarországon az 1970-es és 1980-as években. (T)error&elhárítás 2017/1-2. pp. 98-101. és Az ujjur terrorizmus háttere (T)error&elhárítás 2015/2.

⁸ Lásd még: Harcba a főellenséggel. Hamvas Béla Kultúrakutató Intézet. Budapest, 2014. vagy Lejárata és bomlasztás. Hamvas Béla Kultúrakutató Intézet, Budapest, 2012.

⁹ Bővebben: A terrorizmus hazai és nemzetközi intézményrendszere. In: Bebesi Zoltán (szerk.): Terrorelhárítási alapismeretek. Dialóg Campus Kiadó, Budapest, 2016. pp. 173-192. és Turizmus és biztonság. In: Gonda Gábor (szerk.): A Kárpát-medence turizmusának aktuális kérdései. Pécsi Tudományegyetem, Szekszárd, 2016. pp. 150-160.

E SZÁMUNK TARTALMA

DR. FARKAS ÁDÁM

A TERRORIZMUS ELLENI HARC, MINT KIEMELT ÁGAZATKÖZI FEGYVERES VÉDELMI FELADAT

A tanulmány célja, hogy a terrorizmus elleni fellépés, mint fegyveres állami feladat hazai szabályozását bemutassa és elemezze. E körben a szerző röviden kitekint a terror-ellenes állami feladatrendszer magyarországi előzményeire és tendenciáira. A tanulmány értékeli a szabályozás jelenlegi helyzetét és javaslatokat fogalmaz meg a fejlesztés lehetséges irányaira nézve. E körben a tanulmány a feladatellátás centralizált megoldásaira és koordinációjára fókuszál, de kitér az ágazatközi jelleg erősítésének opcióira is.

Kulcsszavak: terror elleni fellépés, fegyveres védelem rendszere, katonai védelem, rendészet

SZENTIRMAI PÉTER

AZ UKRÁN VÁLSÁG KATONAI OLDALÁNAK ÚJ KIHÍVÁSAI

Tanulmányomban feldolgozom az ukrán válság katonai oldalát. Ennek előzményeként megvizsgálom a nemzetközi biztonságpolitikai környezetet, jogelméleti háttérrel, amely a beavatkozásra hatással lehetett. Részletesen ismertetem a kelet-ukrajnai felkelés kitörését, az orosz csapatok beavatkozásának okait és céljait. Bemutatom a harcok gazdaságra gyakorolt hatását. Feltárom a harcok civilekre gyakorolt hatását, a harcoló felek humánerőforrás bázisát, illetve a civil lakosság manipulálásának az eszközeit. A médiára fókuszálva ismertetem annak felhasználását az ukrán és a szeparatista-orosz oldalról egyaránt. Bemutatom a harctevékenységet, az aszimmetrikus hadviselés alkalmazott elemét. A konfliktuson keresztül fókuszba helyezem a hibrid hadviselés kérdéskörét, és a hálózat alapú hadviselést. Elemzem az orosz fegyverszállításokat, az indirekt és direkt módszerek szimultán alkalmazását a veszteségek és elért eredmények tükrében, valamint a NATO jelenlegi reagáló képességét a hibrid hadviselésre. Ezeket értékelve végső következtetésképp felvetem Magyarország és a NATO jövőbeni aszimmetrikus, képességfejlesztési feladatait, amelyet kiber-, dezinformációs és nemzetbiztonsági szempontokból ellenállóvá kell tenni a kognitív térből érkező támadásokkal szemben.

Kulcsszavak: aszimmetrikus, hibrid, média, hálózat, hadviselés, direkt, indirekt, kiber, dezinformáció, NATO, kognitív, dezinformáció, nemzetbiztonság

CONTENTS

ÁDÁM FARKAS DR.

FIGHTING TERRORISM AS AN IMPORTANT INTER-BRANCH ARMED SECURITY TASK

The study aims to introduce and analyse the domestic regulation of the fight against terrorism as a national security function. The author takes a short outlook on the history and tendencies on national anti-terrorism functions. The study evaluates the current status of the regulations and formulates suggestions considering the possible directions of development. The study focuses on the centralized solutions of task fulfilment, however also touches the possibilities of cross-sector aspect enhancement.

Keywords: counterterrorism, system of armed security, military defense, law enforcement

PÉTER SZENTIRMAI

NEW MILITARY CHALLENGES OF THE CRISIS IN UKRAIN

In this study the military aspect of the crisis in Ukrain is evaluated. First the international security policy environment and the legal background is examined, which may all have had an effect on the intervention. The author elaborates on the East-Ukraine uprising, the aim and cause of the intervention of the Russian troops in detail. The effects the conflict has on the economy and the civilians are presented and also the human resources of the conflicts and the techniques of manipulation. The use of media is introduced both from the Ukrainian and the separatist Russian point of view. Through the conflict the question of hybrid and network based warfare is placed in focus. Russian weapon supplies are analysed and the simultaneous application of direct and indirect methods in the light of the achieved results and also losses. Furthermore, NATO's response ability to hybrid warfare is detailed.

Keywords: assymetric, hybrid, media, network, warfare, cyber, desinformation, NATO, cognitive, national security

CSER ORSOLYA

A MAGYAR NEMZETI BANK HOVÉDELMI ÁGAZATI FELADATAI

Magyarország gazdasági és pénzügyi rendszerének stabilitása és ellenállóképessége fontos nemzeti érdek és biztonságpolitikai szempont – elengedhetetlenné vált a biztonság politikai, katonai, gazdasági, pénzügyi és társadalmi dimenziójának együttes kezelése. Egyre inkább előtérbe kerülnek azon biztonságpolitikai kihívások, melyek kezeléséhez átfogó és összehangolt politikai, gazdasági és katonai fellépésre van szükség. Hazánk elsősorú biztonsági érdeke az ország gazdasági stabilitásának és fejlődésének biztosítása – a felkészülés arra, hogy térségünkben a legfőbb veszélyforrás a gazdasági, pénzügyi, energiabiztonsági, ellátási és környezeti veszélyeztetettség –, összességében az asszimmetrikus hadviselés elleni védelem a meghatározó. Ennek okán alapvető biztonságpolitikai cél a gazdasági és pénzügyi stabilitás folyamatos erősítése és felügyelete, a makroprudenciális szabályozás (rendszerszintű kockázatok folyamatos monitorozása és minél hatékonyabb kezelése) erősítése, a nemzetgazdaság külső kockázati kitettségének csökkentése, a társadalom jólétének megalapozott, biztonságos és hosszú távú erősítése. A Kormány felkérte a Magyar Nemzeti Bank elnökét, hogy szakterületét érintően működjön együtt az MNB-re vonatkozó honvédelmi intézkedési terv kidolgozásával és bevezetésével összefüggő feladatok végrehajtásában, mindazonáltal az üzletmenet folyamatosságának biztosításában.

Kulcsszavak: biztonság, üzletmenet folytonossága, Nemzeti Biztonsági Stratégia, asszimmetrikus hadviselés, pénzügyi stabilitás, makroprudenciális szabályozás

DEÁK VERONIKA

BIZTONSÁGTUDATOSSÁG AZ INFORMÁCIÓS KÖRNYEZETBEN

Napjainkban a biztonságtudatosság nélkülözhetetlen eleme életünknek, hiszen jelenleg egy információs társadalomban élünk, és naponta követnek el kibertámadásokat a különféle bizalmas információk megszerzése érdekében. Ha egy rendszer védett, akkor ezek a támadások leginkább a humán tényezőt érintik, a különböző kihasználható emberi tulajdonságok miatt.

A különféle belső és bizalmas információk megszerzését célzó támadások egyik válfaja a social engineering, amely az emberi tényező befolyásolására, manipulálására, valamint kihasználható tulajdonságaira épít. A támadások célpontja az ember, így hatékony védelem csak a biztonságtudatosság növelésével valósulhat meg, amelynek nélkülözhetetlen eleme a különböző támadási formák, módszerek ismerete.

Jelen tanulmányban az ilyen lehetséges támadások módszereit mutatom be, amelyek ismeretében védettebbek lehessünk a social engineering támadások ellen. A tanulmány részét képezi a felsőoktatási hallgatók körében elvégzett, social engineering eljárást felhasználó kísérlet, amelynek keretében kihelyezésre került egy egyetemi logóval ellátott fadoboz „Telefontöltő” felirattal, amelybe a hallgatók telefonjának megfelelő USB kábelek csatlakoztathatóak. A felmérés azt vizsgálta, hogy a hallgatók milyen arányban csatlakoztatták okostelefonjaikat egy idegen eszközhöz. A kutatás célja az volt, hogy felmérjem a hallgatók biztonságtudatosságát, és rávilágítsak az esetleges hiányosságokra, amelyek a biztonságtudatosság megfelelő fejlesztésével bizonyos szinten orvosolhatók.

Kulcsszavak: social engineering, kibervédelem, biztonságtudatosság, információbiztonság, emberi tényező, humán alapú támadások, IT alapú támadások

ORSOLYA CSER

THE NATIONAL DEFENSE PLAN OF THE HUNGARIAN NATIONAL BANK

The stability and resilience of the economic and financial system in Hungary is an important national interest and security policy aspect – the political, military, economic, financial and social dimension of security have to be handled together. Challenges to security policy are increasingly emphasized, which require comprehensive and coordinated political, economic and military action. The first security concern of our region is to insure the stability and development of our economy, to be prepared that the most vulnerable are the economical, financial, energy safety sectors. Therefore the most important is security against asymmetric warfare. For this reason, a fundamental security policy objective is to continuously strengthen and supervise economic and financial stability, to strengthen macro-prudential regulation (systematic risk monitoring and better management), to reduce the external risk exposure of the national economy, to secure the well-being of society, for a long-term. The Government invited the President of the National Bank of Hungary to cooperate in the field of its speciality in implementing the tasks related to the elaboration and implementation of the National Defense Plan of the MNB, but to ensure the continuity of business.

Keywords: safety, business continuity, National Safety Strategy, asymmetric warfare, financial stability, macroprudential regulation

VERONIKA DEÁK

SECURITY AWARENESS IN AN INFORMATION ENVIRONMENT

Nowadays, security awareness is an essential part of our lives, because now we live in an information society, and cyber-attacks are committed daily in order to obtain a variety of confidential information. If a system is protected, these attacks affect mostly the human factor, because of the different exploitable human behaviour.

Attacks aimed at the acquisition of various internal and confidential information is social engineering, which builds on influencing, manipulating and exploiting the human factor. The aim of the attacks is the human factor; therefore effective protection can only be achieved by increasing security awareness, where knowledge of various forms and methods of attacks is an essential component.

In this study the methods of such possible attacks are presented, and also opportunities for adequate protection against them.

A part of the study is based on research carried out among students in higher education, in which a wooden box was placed with the university logo and "Phone Charger" label, where students could connect their USB cables suitable for their phones. The survey examined to what extent the students connected their smartphones to an unknown device. The aim of the research was to assess the security awareness level of the students, and highlight possible gaps, which can be remedied on a certain level by developing security awareness.

Keywords: social engineering, cyber defence, security awareness, information security, human factor, human-based attacks, IT-based attacks

GULYÁS ATTILA

KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA

A Koreai Népi Demokratikus Köztársaság kiberképességét a rendelkezésre álló információk szűkös mennyisége miatt csak megbecsülni lehet, hiszen az ország politikai berendezkedéséből adódóan az erős cenzúra jelentősen korlátozza az információáramlást, azonban a szomszédos országok hírszerzési információi, a külföldre szökött tisztviselők beszámolóit, valamint az országhoz köthető kibertámadások elemzéseit megalapozzák azt a feltételezést, miszerint Észak-Korea az elmúlt közel két évtizedben olyan magas szintre fejlesztette kiberképességét, hogy helyet követelhet magának a nemzetközileg elismert kiberhadviselő országok élmezőnyében.

Kulcsszavak: Észak-Korea, Koreai Népi Demokratikus Köztársaság, Lazarus, kibertámadás, Novetta, Blockbuster, Operation Flame, Operation I.Mission, Operation troy, Dark Seoul 2013, MYDOOM, Dozer, Operation Troy, Ten days of rain, NewRomantic Cyber Army, Whols Hacking Team, Bluenoroff, SWIFT, Sony

FINK NÁNDOR – HORVÁTH CSONGOR MÁRK

A SZOLGÁLTATÓ ROBOTIKA HELYZETE ÉS KUTATÁSI IRÁNYAI

A robotika dinamikus fejlődése az elmúlt években folyamatos erős növekedést mutatott és az előrejelzések szerint további jelentős beruházások várhatóak e téren. Napjaink széleskörű, de célfeladatokat ellátó hadi vagy ipari robotok mellett bővül a robotizálható feladatok köre, így a mindennapi életben az otthoni és intézményi alkalmazásaikkal is találkozhatunk. Jelen írás célja, hogy egy rövid áttekintést adjon a robotikai piac jelenlegi helyzetéről és a következő pár évben várható átalakulásáról. Nagyobb hangsúlyt szentelünk a szolgáltató robotikára, mely jelenleg is intenzív kutatás alatt álló terület és a hétköznapi használat meghatározó részét fogja képezni, valamint az ipari és biztonsági/műveleti környezetben is létjogosultsággal bír, főleg a kis és középvállalatok (KKV), valamint alegység szintű alkalmazás esetén.

A szolgáltató robotokkal kapcsolatban kitérünk az ember-robot interakcióra, a közös térben való tartózkodáshoz szükséges érzékelés kibővítésére irányuló kutatásokra, továbbá a robotok zárt térben való tájékozódására és pályatervezésére, valamint az etorobotika bemutatására és az eddig elért eredmények rövid ismertetésére.

Kulcsszavak: Katonai robotok, Szolgáltató robotok, Távműködtetés, Etorobotika, Intelligens terek

ATTILA GULYÁS

CYBER WARFARE IN A NORTH-KOREAN WAY

The cyber capacity of the Democratic People's Republic of Korea can only be estimated due to the scarce available information, as the strict censure significantly narrows down the information flow. However, the intelligence information of the neighbouring countries, the accounts of the defectors from North Korea and the evaluations of the cyber attacks linked to the country all ground the assumption, that in the last two decades North Korea has developed its cyber capabilities in an increasing scale and capacity. The country might be even able to demand a place among the internationally acknowledged, most developed cyber superpowers.

Keywords: North-Korea, Democratic People's Republic of Korea, General Staff Department of the Korean People's Army, information warfare, cyber attack, cyber strategy, reconnaissance, sabotage, virus, threshold of war

NÁNDOR FINK – CSONGOR MÁRK HORVÁTH

CURRENT STATE AND RESEARCH TRENDS OF SERVICE ROBOTICS

Robotics is a rapidly growing industry and based on future prognoses significant investments are expected in the coming years. It has a high influence on everyday life, thus the area of application extends from industrial and military to the institutional and domestic fields. The main aim of this paper is to give a brief overview of the actualities and the expected trends and changes of the robotics market. Besides military application, a deeper analysis is given on service robotics due to its highlighted role in the recent state-of-the-art research and importance in everyday-, industrial and security/operational environment. In particular, in the application of small and medium sized companies.

Regarding service robotics, the human-machine interactions are touched upon, the research on the augmentation of shared space operations, nevertheless the orientation, navigation and path planning of mobile robots in an in-door environment. In the last section, a short overview is given about the etho-robotics, its importance and the results achieved in this unique area.

Keywords: Military robotics, Service robotics, Remote manipulation, Ethorobotics, Intelligent Space

KOVÁCS KRISZTIÁN

HAZEN AMES TÖRTÉNETE I.

A tanulmány nyílt dokumentumok alapján mutatja Aldrich Hazen Ames volt titkosszolgálati tiszt kémtevékenységét és ezen keresztül azt, hogy az amerikai Központi Hírszerző Ügynökség (CIA) hogyan integrálta az elhárító tevékenységet a hírszerző szervezet struktúrájába. Bepillantást nyerhetünk a CIA vizsgálati eljárásrendjébe, megismerkedhetünk a szervezeti kultúrával, amelynek diszharmóniája az alkalmazott elhárító tevékenységgel, súlyos következményekkel járt. Az Ames kémügy adalékokkal szolgál a magyar katonai hírszerzés tevékenységével kapcsolatban is.

Kulcsszavak: elhárítás, hírszerzés, CIA, nemzetbiztonsági rendszer, Clyde Lee Conrad, Belovai István

DR. GYARAKI RÉKA

JOGI SZABÁLYOZÁS A NEMZETI ELEKTRONIKUS ADATVAGYON, AZ AZT KEZELŐ INFORMÁCIÓS RENDSZEREK, LÉTFONTOSSÁGÚ INFORMÁCIÓS RENDSZEREK ÉS RENDSZERELEMEK BIZTONSÁGÁRÓL

A XXI. század globális kihívásai közé tartoznak a kibertérből érkező támadások, amelyek irányulhatnak a nemzeti adatvagyon vagy a kritikus információs infrastruktúrák ellen. „A technológiai fejlődés és az információs igények globalizálódása, az egyre nagyobb intenzitású és egyre veszélyesebb – többek között a kritikus infrastruktúrákat is érintő – fenyegetések megkövetelik a honvédelmi feladatokhoz kapcsolódó kibervédelmi helyzet áttekintését és a szükséges feladatok meghatározását és végrehajtását.”

A tanulmányban az információbiztonsággal kapcsolatos feladatokat és azokat az intézményeket tekintem át, amelyek többek között a nemzeti adatvagyonnal, valamint a létfontosságú információs rendszerekkel kapcsolatba hozható intézmény, így a Nemzeti Kibervédelmi Intézet, a Katonai Nemzetbiztonsági Szolgálat, valamint a Magyar Honvédség kibertámadásokkal kapcsolatos tevékenységét és hazai jogi szabályozását.

Kulcsszavak: honvédség, nemzetbiztonság, nemzeti adatvagyon, kritikus információs infrastruktúra, kiberbiztonsági stratégia

KRISZTIÁN KOVÁCS

THE STORY OF ALDRICH HAZEN AMES, PART I.

The study, based on open source documents, introduces the espionage activity of Aldrich Hazen Ames former intelligence officer and through his activity how the Central Intelligence Agency integrated counterintelligence activity into the structure of an intelligence agency. We can get an insight into the operational procedures and get familiar with the organizational culture, which was in disharmony with the applied counterintelligence activity. This however had serious results. The Ames case serves with interesting addition to the Hungarian military intelligence activity as well.

Keywords: counterintelligence, intelligence, Central Intelligence Agency (CIA), Clyde Lee Conrad, István Belovai

RÉKA GYARAKI DR.

LEGAL REGULATION ON THE SECURITY OF NATIONAL ELECTRONIC DATA ASSETS, INFORMATION SYSTEMS MANAGING THEM AND OF CRUCIAL INFORMATION SYSTEMS AND SYSTEM ELEMENTS

In the 21st century attacks from the cyberspace have become a global issue. These attacks aim at our national data assets or critical information infrastructures. The technological development and the globalization of information demands, the more and more intense and more dangerous threats – which can affect the critical infrastructures – all demand the overview of cyber protection tasks connected to national defense, the determination and execution of the necessary tasks in this regard. In this study I will review the tasks of national defense, the work of the National Cyber Security Center, the Military National Security Service and the Hungarian Defense Forces regarding cyber attacks and the Hungarian legal regulations. The task of national defense is to protect from external attacks, which nowadays can be performed not only with weapons, but thanks to cyber threats – cyber terrorism and cyber warfare – the defense forces have to be able to protect without weapons, too.

Keywords: army, national security, national data asset, critical information infrastructure, cyber security strategy

MAKAY MÁTYÁS

A RACIONÁLIS GONDOLKODÁS KÉPESSÉGÉNEK KVANTITATÍV MÉRÉSE

A publikáció a racionalitás szűkebb, ismeretelméleti fogalmával és az ilyen módon értelmezett racionális gondolkodás jellemzőivel foglalkozik. Az írás központi gondolata, hogy a racionális gondolkodás képessége az intelligenciától világosan megkülönböztethető kognitív képesség, fontosságát pedig az adja, hogy döntő hatással bír gondolkodásunk hatékonyságára. A tanulmány kiemelt témája a racionalitás kvantitatív mérésének legújabb eredményei, aminek keretén belül részleteiben foglalkozik a Keith Stanovich által vezetett amerikai kutatócsoport által elkészített RQ (racionalitás-hányados) teszttel és annak magyar változatával az elméleti alapok és az első tapasztalatok tükrében. Lényeges szempontok kerülnek megemlítésre az RQ-teszt gyakorlati használatáról a kiválasztási folyamatban, illetve a meglévő munkatársak körében.

Kulcsszavak: intelligencia, racionalitás, racionális gondolkodás, racionális gondolkodás mérése, RQ, racionalitás-hányados, RQ teszt, kognitív torzítás, kognitív torzítások csökkentése

MÁTYÁS MAKAY

QUANTITATIVE MEASUREMENT OF RATIONAL THINKING

The article explores the concept of epistemic rationality and the characteristics of rational thinking. Its focal idea is that rationality is a separate cognitive ability, so that it is not included in intelligence, and that rationality has an immense effect on efficient thinking. The central topic is the latest findings in the field of quantitative measurement of rational thinking. There is a comprehensive review of the RQ (Rationality Quotient) test prototype presented recently by the research team of Keith Stanovich and also that of the Hungarian version of the test. Important points are articulated concerning the practical use of the RQ test in the selection process and also in the training of staff members.

Keywords: intelligence, rationality, rational thinking, measuring rationality, RQ, rationality quotient, RQ test, cognitive bias, cognitive debiasing

SZERZŐINK

Cser Orsolya	HM Védelmi Igazgatási Főosztály Központi Koordinációs Osztály szakreferense
Deák Veronika	Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, PhD hallgatója
Dr. Dávid Ferenc	Nemzeti Közszolgálati Egyetem Katonai Nemzetbiztonsági Tanszék, egyetemi adjunktusa
Dr. Farkas Ádám	Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Vezetőképző Intézet Honvédelmi Jogi és Igazgatási Tanszékének tanársegédje
Fink Nándor	Budapesti Műszaki és Gazdaságtudományi Egyetem, Gépészmérnöki Kar, Mechatronika, Optika és Gépészeti Informatika Tanszék, PhD hallgatója
Gulyás Attila	nyá. alezredes
Dr. Gyaraki Réka	őrnagy, Nemzeti Közszolgálati Egyetem Rendészetudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék, tanársegéd
Horváth Csongor Márk	Budapesti Műszaki és Gazdaságtudományi Egyetem, Gépészmérnöki Kar, Mechatronika, Optika és Gépészeti Informatika Tanszék, PhD hallgatója
Kovács Krisztián	alezredes, a KNBSZ munkatársa
Makay Mátyás	Eötvös Loránd Tudományegyetem, Pszichológia Doktori Iskola, PhD hallgatója
Szentirmai Péter	Nemzeti Közszolgálati Egyetem MSc hallgatója, okl. biztonsági és védelempolitikai szakreferens

E SZÁMUNKAT LEKTORÁLTÁK

Árpád Zoltán	ezredes, a KNBSZ munkatársa
Bálint Tamás	alezredes, a KNBSZ munkatársa
Prof. em. Dr. Bolgár Judit	ny. ezredes, CSc, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi tanár
Dr. Fürjes János Norbert	alezredes, PhD NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
Dr. Kádár Pál	PhD, dandártábornok, HM Tervezési és Koordinációs Főosztály vezetője
Dr. Kassai Károly	ezredes, a KNBSZ munkatársa
Dr. Kenedli Tamás	ezredes, PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
Dr. Király László	CSc, a hadtudomány kandidátusa, az MHTT alelnöke, a Védelemgazdasági és Logisztikai Szakosztály elnökségi tagja
Dr. Korondi Péter	PhD, Budapesti Műszaki és Gazdaságtudományi Egyetem, Gépészmérnöki Kar, Mechatronika, Optika és Gépészeti Informatika Tanszék vezetője
Kővári László	alezredes, a KNBSZ munkatársa
Dr. Magyar Sándor	ezredes, PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék, adjunktus, a KNBSZ munkatársa
Dr. Sabjanics István	főhadnagy, PPKE JÁK Nemzetközi Közjog Tanszék, tudományos segédmunkatárs, a KNBSZ munkatársa
Simon László	alezredes, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
Szabó Károly	ezredes, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
Tóth Csaba Mihály	alezredes, a KNBSZ munkatársa

A SZAKMAI SZEMLÉBEN TÖRTÉNŐ PUBLIKÁLÁS FELTÉTELEI

Az írásművekkel szemben támasztott követelmények

Etikai követelmények:

- az írásmű másol, 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 területkétemáit, 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 megjelenítésre, 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 jegyzetben²⁹⁹ módszerrel kérjük alkalmazni.

Abban az esetben, ha a szerző nem ezt a módszert alkalmazza, a kéziratot lektorálás nélkül visszaküldjük átdolgozásra!

Idézetek 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.

²⁹⁹ 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.³⁰⁰

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

³⁰⁰ Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. p. 18.