

*Dr. Dávid Ferenc: Nemzeti biztonság és nemzetbiztonság
a stratégiaalkotásban*

Dr. Gyömbér Béla: Rivalizáció a kádári hírszerzésben

*Dr. Jávor Endre: A hír, az adat, az információ és a
dokumentáció fogalma, helye, szerepe a döntéshozatalban*

*Sági Gábor: Practical Issues of IT Security Incident Handling
in Market Environment and in Public Administration*

*Drusza Tamás: A nemzetbiztonsági stratégiáról
a Nemzeti Katonai Stratégia tükrében*

*Simon László – Dr. Magyar Sándor: A terrorizmus
és indirekt hatása a kiberterében*



NEMZETBIZTONSÁGI SZEMLE

A Nemzeti Közzolgálati Egyetem
Nemzetbiztonsági Intézetének
elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756

V. évfolyam, 3. szám, 2017.

A szerkesztőbizottság elnöke: Dr. Boda József, NKE

Főszerkesztő: Dr. Dobák Imre, NKE

Szerkesztő: Dr. Deák József, NKE

Internetes megjelenés: Dr. Pétery Kristóf, NKE

Internetes elérhetőség: <http://nbszemle.uni-nke.hu>

Szerkesztőség: Nemzeti Közzolgálati Egyetem, Nemzetbiztonsági Intézet
1101 Budapest, Hungária krt. 9-11.

Levelezési cím: Nemzeti Közzolgálati Egyetem, Nemzetbiztonsági Intézet
1581 Budapest, Pf.: 15.

E-mail: nbszemle@uni-nke.hu

Szerkesztőbizottság

Elnöke: Dr. habil. Boda József
Tagok: Dr. Béres János
Dr. Botz László
Dr. Dobák Imre
Hazai Lászlóné dr.
Dr. Kobolka István
Dr. Kovács Zoltán András
Prof. Dr. Padányi József
Dr. Regényi Kund Miklós
Dr. habil. Resperger István
Prof. Dr. Szakály Sándor
Dr. Takács Tibor
Dr. Vida Csaba

Kiadó:

Nemzeti Köszolgálati Egyetem
1101 Budapest, Hungária krt. 9-11.

E számunk szerzői:

Dr. Dávid Ferenc NKE

Dr. Gyömbér Béla

Dr. Jávor Endre

Sági Gábor

Drusza Tamás NKE

Simon László NKE

Magyar Sándor NKE

A számban megjelent írásokat lektorálták:

Dr. Kassai Károly

Dr. Regényi Kund

Dr. Kovács Zoltán

Dr. Zalai-Göbölös Noémi

Dr. Dávid Ferenc

Dr. Dobák Imre

Tartalomjegyzék

Nemzeti biztonság és nemzetbiztonság a stratégiaalkotásban	5
Rivalizáció a kádári hírszerzésben	22
A hír, az adat, az információ és a dokumentáció fogalma, helye, szerepe a döntéshozatalban	36
Practical Issues of IT Security Incident Handling in Market Environment and in Public Administration	61
A nemzetbiztonsági stratégiáról a Nemzeti Katonai Stratégia tükrében	77
A terrorizmus és indirekt hatása a kiberterében	89

Nemzeti biztonság és nemzetbiztonság a stratégiaalkotásban

Dávid Ferenc¹

Absztrakt:

A rendszerváltozást követően a magyar állam biztonsági gondolkodását biztonság- és védelempolitikai alapelvei határozták meg. Ez alapjául szolgált az ezredfordulót követően megjelent, módosított és újrafogalmazott nemzeti biztonsági stratégiának. Az első nemzeti biztonsági stratégia lényeges eleme, hogy utalást tett a származtatott ágazati stratégiák és utóbbi részeként egy ún. „nemzetbiztonsági stratégia” kidolgozására. S bár ágazati iránymutatás nem készült a nemzeti biztonsági stratégia hangsúlyozza a hírszerzés és elhárítás szolgálatok fontosságát. A tanulmány célja, hogy a biztonsági gondolkodásban, Magyarország biztonság- és védelempolitikájában, nemzeti biztonsági rendszerében elhelyezze a nemzetbiztonsági szolgálatokat és felvázolja azokat az irányokat, amelyek a rendszerváltozást követően meghatározóak voltak a magyar stratégiaalkotásban. (A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Egyed István Posztdoktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.)

Kulcsszavak: nemzetbiztonság, nemzeti biztonság, stratégiaalkotás

Abstract:

The Hungarian security thinking was defined by its security and defense policy principles following the political transformation. This served as a basis for the published, modified and redefined national security strategy after the millennium. The essential element of the first Hungarian national security strategy was that it referred to a derivative and sectorial “national security” strategy. Although a sectorial guidance was never drafted the national security strategy emphasizes the importance of intelligence and counter-intelligence. The purpose of this study is to specify the place of national security services in security thinking, in Hungarian security and defense policy and its national security order and outline the directions of strategy making after the political transformation. („The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the István Egyed Postdoctoral Program.”)

Keywords: national security, strategy making

¹ Dávid Ferenc dr. jur., Ph.D., Nemzeti Közszolgálati Egyetem, egyetemi adjunktus, david.ferenc@uni-nke.hu, ORCID azonosító: orcid.org/0000-0003-0570-2899

Bevezetés

Napjaink változó világában nem lehet mindenre felkészülni és ez a gondolkodás az elmúlt évtizedek „kockázat-társadalom” víziójának elfogadásában is megjelent, de kiemelt jelentősége van a mindenkori kormányzat iránymutatásának, ami kijelöli a szervezetrendszer alkotóelemei által ellátandó feladatokat, elhatárolja a hatásköröket, megteremti a feladatteljesítéshez szükséges forrásokat. Az állam (nemzet) biztonsága egy elvont elméleti fogalom, amit összetettségén, tartalmi mélységén és szubjektív alkotóelemein keresztül értelmezhetünk és származtatjuk belőle a nemzetbiztonsági szolgálatok feladatrendszerét.

A rendszerváltozást követően a magyar állam biztonsági gondolkodását biztonság- és védelempolitikai alapelvei határozták meg, ami alapjául szolgált az ezredfordulót követően megjelent, módosított, majd újrafogalmazott (és a tanulmány megjelenése idején ismét napirendre került) nemzeti biztonsági stratégiának. Az elmúlt évtizedek jellegzetessége, hogy a magyar stratégiaalkotási folyamatban a klasszikus biztonság- és védelempolitikai szemlélet mellett az ország szempontjából releváns értékek és érdekek, valamint hatályos jogszabályi háttér mentén vezették le a nemzetbiztonsági szférára háruló feladatokat. Először 1993-ban, majd 1998-ban adták ki a magyar biztonsági dokumentumok alapjának tekintett biztonság- és védelempolitikai alapelveket. Az ezredfordulót követően elfogadott nemzeti biztonsági stratégia lényeges eleme, hogy 2002/2004-től hatályos formában utalást tett a származtatott ágazati stratégiák és utóbbi részeként egy ún. „nemzetbiztonsági stratégia” kidolgozására, ami egy nem elhanyagolható folyamat részeként vezetett el a napjainkban is tartó szakmai diskurzushoz. S bár ágazati iránymutatás nem készült, a 2002-ben elfogadott, 2004-ben módosított, majd 2012-ben újrafogalmazott² nemzeti biztonsági stratégia nevesíti és deklarálja a hírszerzés és elhárítás szolgálatok fontosságát.³

A tanulmány célja, hogy a biztonsági gondolkodásban, Magyarország biztonság- és védelempolitikájában, nemzeti biztonsági rendszerében elhelyezze a nemzetbiztonsági szolgálatokat és felvázolja azokat az irányokat, amelyek a rendszerváltozást követően meghatározóak voltak a magyar stratégiaalkotásban.

Nemzet, biztonság és nemzetbiztonság

A rendszerváltozás előtt hivatalosan használt „állambiztonsági szolgálat” és a társadalom szélesebb körében általános értelemben ismert „titkosszolgálat”

² 2144/2002. (V. 6.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról, majd 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság (új) nemzeti biztonsági stratégiájáról és a jelenleg hatályos 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

³ Lásd: 1035/2012. (II. 21.) Korm. határozat 48. p.

szavunkat a jogalkotó a politikai átmenetet részeként, mint „nemzetbiztonsági szolgálat” definiálta. Az állam vagy a politikai értelemben vett nemzet biztonsága a szolgálatok feladatellátásnak középpontjában áll; még akkor is, ha a nemzetbiztonság szavunk alapjaként értelmezett „nemzet” fogalma folyamatos szakmai viták kiindulópontját képezte. A szókapcsolat „biztonság” része alapvetően percepció, ami időben és térben változó jelentéstartalommal tölthető meg. A biztonság és biztonságérzetre vonatkozó képzet, jelentős mértékben meghatározza és befolyásolja azokat a politikai-társadalmi súlypontokat, amelyek determinálják a nemzetbiztonsági szolgálatok feladatellátását és működését.⁴

Különleges társadalmi értéként a biztonság nélkülözhetetlen elem a konszolidált állapotok megteremtésében. A társadalmi fejlődés nélkülözhetetlen az állami élet, a nemzetgazdaság, a politikai szféra és a hétköznapi élet zavartalan, fenyegetésektől és veszélyektől mentes működéséhez. A biztonságot a társadalom és az állam zavartalan működésének keretfeltételeként is meghatározhatjuk, ahol az egyes szolgálatok rendeltetésszerű működése során a közösség tagjai alig vagy nem is érzékelik jelenlétüket. A szféra jelentőségére általában a belső rend és biztonság hiányában, vagy zavara esetén figyelnek fel. A biztonság értékőrző és értékteremtő funkciója egyértelműen bizonyítható. A szélesebb értelemben vett fogalom feltétele az ország és a társadalom anyagi, szellemi, kulturális fejlődésének. Megőrzése értéként és érdekként jelenik meg a társadalmi csoportok, egyének életében.⁵

A térben és időben eltérő tartalommal megtölthető biztonság a társadalom tagjainak alkotmányos alapvető jogaként is meghatározható. A biztonság megteremtése szempontjából lényeges területek és hangsúlyok az egyén, a közösség és az ország vezetőinek szubjektív értékítélete szerint rendeződhetnek; hangsúlyosságuk szerint rangsorolódnak és együttesen határozzák meg, hogy egy adott állam és közösség milyen tartalommal definiálja a biztonsági egyes területet.

A rendszerváltozás óta eltelt évtizedek és különösen az ezredfordulót követő időszak átformálták a biztonságról és a nemzetbiztonsági szféráról való gondolkodást. A változás és komplex paradigmaváltás alapja, hogy az állam átalakulása magában hordozta az állam biztonságáért felelős szerveinek változását. A nemzetbiztonsági tevékenység központi elemét továbbra is a mindenkori állam belső rendjének, területi integritásának és szuverenitásának védelme és nemzetbiztonsági érdekeinek érvényesítése jelentette.⁶ Magyarország nemzetbiztonsági szolgálatainak a korábbi struktúrák teljeskörű átalakítása mellett kellett a rendszerváltozást követő néhány év alatt felkészülni az új típusú külső és belső fenyegetésekkel szemben.⁷

Megmaradt a klasszikus biztonságfelfogás katonai és politikai eleme, de meg

⁴ Lásd: SIEBER 2016. 14-18. o.

⁵ GAZDAG 2001. 32. o.; IZSA 2009. 22. o.

⁶ 1995. évi CXXV. törvény 74. §; lásd még: KOCIS 2008. 58. o.; IZSA 2009. 11-12. o.

⁷ RÉVÉSZ 2003. 67-68. o.

kellett osztani helyét egy komplex biztonságfelfogás megannyi területével. Eltűnt a korábban definiált stabil ellenségkép és a hivatkozott, könnyen azonosítható cél és átadta a helyét mindazon kihívásoknak, kockázatoknak és fenyegetéseknek, amelyek kezeléséhez a hírszerző és elhárító szolgálatok önmagukban alkalmatlannak bizonyultak. Átalakult a felderítésre, hírszerzésre és elhárításra vonatkozó korábbi gondolkodás és kimunkált eljárási rend,⁸ mert a korábban távolinak és absztraktnak tűnő új típusú biztonsági kihívások hirtelen reális és időszerrű problémaként bukkantak fel. A nemzetbiztonsági szolgálatok beemelték feladatrendszerükbe a globális biztonsági kihívásokat és megteremtették a hazai és nemzetközi együttműködésnek és a veszélyek elhárításának lehetőségét is.

A rendszerváltást követően megindult egy stratégiaalkotási folyamat Magyarországon, ami egy modern biztonság- és védelempolitikai szemléletet vezetett be és az ország szempontjából releváns értékek és érdekek mentén vezette le a nemzetbiztonsági szolgálatokra háruló feladatokat.⁹ A jogalkotó már a '90-es évek kezdetén, a nemzetbiztonsági törvény 1995-ös elfogadásával megfogalmazta a szűkebb értelemben vett nemzetbiztonsági érdeket, amit a legutóbbi transzformációs években emeltek alaptörvényi szintre. A fogalmat legszűkebb értelemben, mint a Magyar Köztársaság, majd Magyarország szuverenitásának biztosításában és alkotmányos rendjének védelmében és nemzetbiztonsági érdekeinek érvényesítésében határozta meg. Tágabb értelemben a nemzetbiztonsági törvény, értelmező rendelkezése és tartalmi kibontása a célkitűzések szélesebb körű regiszterét foglalta magába. Alapkövetelmény volt az ország függetlensége és területi épsége elleni támadó szándékú törekvések felderítése, az ország politikai, gazdasági, honvédelmi érdekeit sértő vagy veszélyeztető leplezett törekvések felderítése és elhárítása. A jogszabály kiemelten kezelte a kormányzati döntéshozatal döntéseihez szükséges, a külföldre vonatkozó, illetőleg külföldi eredetű információk megszerzését. Az euroatlanti térség célkitűzéseivel és hazánk csatlakozási törekvéseivel összhangban fontos volt a demokratikus értékek általános érvényesülésének és érvényesítésének biztosítása. Ennek keretén belül vált meghatározó feladattá az alapvető emberi jogok gyakorlását biztosító alkotmányos rend, a többpártrendszeren alapuló képviselői demokrácia és az alkotmányos intézmények működésének törvénytelen eszközökkel történő megváltoztatására vagy megzavarására irányuló leplezett törekvések felderítése és elhárítása. Az új típusú globális fenyegetések által hordozott biztonsági kockázat alapján a törvényhozó kiemelten kezelte a terrorcselekmények, az illegális fegyver- és kábítószer-kereskedelem, valamint a nemzetközileg ellenőrzött termékek és technológiák illegális forgalmának felderítését és megakadályozását.¹⁰

A jogalkotó által szűkebb és tágabb értelemben megfogalmazott (állam- és nemzetbiztonsági érdek a gyorsan változó világban kijelölte a feladatellátás

⁸ LÉNÁRT 2007. 36-37. o.

⁹ IZSA 2009. 139-141. o.

¹⁰ GÁL 2014. 43-74. o.; 1995. évi CXXV. törvény 74. § a) bekezdés

alappilléreit, amiből minden további nemzetbiztonsági feladat származtatott. Az 1990-es évek jogalkotói tevékenységének utólagos méltatása a rendszerváltozás óta eltelt idő múlása, mert évtizedekre megteremtette a nemzetbiztonsági szolgálatok feladatellátásnak kereteit.¹¹ A törvényhozás és végrehajtás (kormányzat) felelőssége, hogy a jogszabályokban és a stratégiai dokumentumokban megfogalmazott irányok mentén meg lehessen határozni a nemzetbiztonsági szféra előtt álló feladatokat és összpontosítani lehessen az erőforrásokat. Egyik oldalon az egymás hatását erősítő biztonsági kihívások dinamizmust kölcsönöznek a folyamatoknak. A másik oldalon az arányaiban korlátozottabb, de megfelelően definiált és összpontosított erőforrások, súlypontok kialakítását követelik meg a nemzetbiztonsági szférától.

Az állam (nemzet) biztonsága egy elvont elméleti fogalom, amit összetettségén, tartalmi mélységén és szubjektív alkotóelemei során keresztül lehet értelmezni. A jogállam optimális esetben egy, a jog talaján álló struktúra szabályain keresztül és egyedi logika mentén működő rendszerként határozható meg, de a fentiekből egyenesen következik, hogy a biztonság megteremtése csak (állam-) cél. A társadalom biztonságérzete az egyének szubjektív érzéseként határozható meg, de ez közelről sem jelenti az objektív biztonság meglétét. Nincs abszolút biztonság. Az állam a (nemzet) biztonság fogalmának tartalma alatt azért felel, hogy lehetőségeihez képest megtett-e mindent az állami célkitűzés megvalósítása érdekében. Egy alternatív biztonságfelfogás alapján a biztonság egy kívánt állapot, absztrakt államcél, amelyben az állam és a társadalom értékei nincsenek veszélyben, érdekeinek sérelme nem valószínű. Ez a szint védelemmel érhető el, ahol a védelem egyes részterületei egymással összekapcsolódnak. A biztonság nem az egyes értékek, vagy érdekek védelmét jelenti, hanem egy komplex, a szervezet oldaláról való megközelítési módot; a védelmi erőfeszítéseket rész és egész tekintetében egyszerre kell kifejezni. Az állami intézményrendszer és nemzetbiztonsági szolgálatok feladata, hogy a biztonság, mint államcél megvalósítása érdekében a feladatkörök mentén időben és térben valós súlypontokat képezzenek.¹²

A biztonsági környezet hangsúlyai

Az európai kontinens kelet-nyugati megosztottsága és Magyarország biztonsági környezetének megváltozása meglepő gyorsasággal ment végbe a rendszerváltozáskor. A magyar transzformációs időszak a társadalmi, gazdasági és politikai élet minden területén érezte hatását. A változás előestéjén állambiztonsági szféra

¹¹ Összehasonlítva az 1990. évi X. törvény és a 26/1990. (II. 14.) MT rendelet „átmeneti” rendelkezéseivel, az 1995. évi CXXV. törvény átfogó és hosszútávú megoldásnak bizonyult; az állítás még akkor is igaz, ha bizonyos időközönként felvetődik megújításának igénye.

¹² FINSZTER 2008. 26. o.; SIMON 2007. 7. o.

nem csak szervezeti oldalról viselte magán a békés átmenet politikai kompromisszumainak nyomát, de a feladatrendszerében meghatározott korábban stabil ellenségkép eltűnt, átalakult, vagy ellentétes előjelet kapott és fokozatosan átadta helyét az absztrakt, és előre nehezen jelezhető fenyegetéseknek.¹³ Az új, összetettebb és átalakult jelentéstartalommal meghatározott feladatok a rendszerváltozást követő évek során egy folyamat részeként kerültek ismét előtérbe és kirángatták a nemzetbiztonsági szférát az önmeghatározási válságból. A klaszikus biztonságfelfogás politikai és katonai elemét a kihívásoknak egy új és összetettebb regisztere váltotta fel, ami a biztonság hagyományos elemei mellett a gazdasági, társadalmi (szociális) és környezeti dimenzióinak fontosságát is igazolta. Hivatkozott új típusú kihívások nem csak, hogy változatosabbak lettek, de kevésbé lehetett őket előre jelezni, megelőzni, elhárítani, vagy káros hatásukat kezelni, ami ismét előtérbe helyezte a hírszerző és elhárító szolgálatok horizont ellenőrző tevékenységét.¹⁴

A nemzetközi rendszer átalakulásának részeként a hagyományos nemzetálami szereplők mellett a mindennapokban egyre nagyobb hatást gyakorolnak az úgynevezett nem-állami szereplők.¹⁵ Az (állam-) nemzetbiztonsági szolgálatok a hidegháború végén egy arányaiban összetettebb biztonsági (és geopolitikai) helyzetben találták magukat. A hagyományos kihívások mellett mind jellemzőbb új típusú, az országhatárokon átívelő fenyegetésekkel szembesültek, amelyeket kevésbé lehetett felismerni és előre jelezni.¹⁶ Napjainkban egy országot és közösséget érő kihívások, kockázatok, fenyegetések többnyire a jog által nehezen elérhető területekről érkeznek, míg háttérükben társadalmi, természeti jelenségek és utóbbiak egymásra hatása húzódhat meg. Mindennapjainkból tudatában vagyunk, hogy a természeti veszélyek tekintetében vállalnia kell egy előre be nem látható kockázatot az elhárítható vagy el nem hárítható erőhatalommal (*vis maior*) szemben. A természeti mozgásokhoz hasonlóan jelenséget produkálhatnak a társadalmi folyamatok is; kezelésük során beszűkülnek az állam/közösség védekezési lehetőségei.¹⁷ A szociális, gazdasági, környezeti stb. veszélyforrások nehezen tarthatók kordában, velük szemben az állami és társadalmi védekezés csak csökkenteni tudja hatásukat. A széles spektrumú kockázati lehetőségekkel szemben még az együttműködés keretei között is csak aránytalanul kisebb nemzeti védekezési lehetőséggel számolhatunk. Utóbbi miatt szükséges, hogy adott közösség vagy szervezetrendszer felismerje és azonosítsa az adott időben és térben meghatározó fenyegetéseket és utóbbiakból származtatott feladatokat.¹⁸

¹³ IZSA 2009. 142. o.

¹⁴ GAZDAG 2001. 34. o.; TÓTH 2011. 114. o.

¹⁵ Lásd: nemzetközi szervezetek, multinacionális vállalatok, nem kormányzati szervezetek, nemzetközi szervezett bűnözői és terrorista csoportok stb.

¹⁶ IZSA 2009. 142. o.

¹⁷ FINSZTER 2008. 25-26. o.

¹⁸ MATUS 2012. 54-55. o.

Napjaink globális fenyegetései nem ismerik az állami határokat, utóbbi pedig megnehezíti és mégis alapja a közös fellépésnek. A jövő tekintetében folyamatosan számolni kell az egymás hatásait erősítő biztonsági problémák együttes jelentkezésével, relatíve az egyik pillanatról a másikra történő megjelenésével. Egy absztrakt (szubjektív) biztonsági szint elérése érdekében mind lényegesebbé válnak az együttműködés különböző formái. Ez részben a magyar állam biztonságáért felelős szervei együttműködésének szükségességét, másrészt a szövetséges/külföldi államok partnerszolgálataival történő két- és többoldalú kapcsolatok fontosságát jelenti. Napjainkra egyértelmű, hogy a Magyarországot érintő biztonsági kihívások csak egy közös érdekek mentén szervezett együttműködés keretében kezelhetők, amihez szervezeti alapot az ország szövetségi, közösségi és más nemzetközi együttműködési formái kínálnak.¹⁹

Megállapíthatjuk, hogy a biztonságról alkotott fogalmunk és gondolkodásunk a rendszerváltást megelőző évtizedektől kezdve átalakult. Nem számolhatunk állandó és kiszámítható fejlődési ívvel, nincsenek általános szabályok, vagy hosszú távú regiszterek, ami minden lehetséges biztonsági kockázatot és forgatókönyvet számba vesz.²⁰ A nemzeti biztonsági stratégia célja, hogy regiszter és sorvezető legyen, összefoglalja az állam biztonságát veszélyeztető elemeket. Az elmúlt évtizedek változásai feloldották a külső és a belső biztonság, az állam és a magánszektor, a prevenció és a represszió, valamint az ezekhez korábban egyenként hozzárendelhető, elkülönült eszközöket és szervezeteket. Nincsen élesen szétválasztható szervezetrendszer és hozzárendelt feladat, ahogy önmagában kezelhető biztonsági probléma sem létezik.

A biztonság- és védelempolitikai alapelvektől a stratégiáig

Napjaink változó világában – bár nem lehet mindenre felkészülni – mégis kiemelt jelentősége van a kormányzati iránymutatásnak, ami kijelöli az intézmények által ellátandó feladatokat, elhatárolja a hatásköröket, megteremti a feladatteljesítéshez szükséges megfelelő jogszabályi háttérrel és rendelkezésre bocsátja a szükséges forrásokat. Megvizsgálva az elmúlt évtizedek stratégiai dokumentumainak iránymutatásait, a kormányzati és szakértői gondolkodás egyértelműen az ún. kockázat-társadalom víziójának elfogadása irányába mutatott.²¹

A tanulmány szempontjából és rendszerváltást követő stratégiai dokumentumok sorában vissza kell nyúlni az előző évezred utolsó évtizedének végéig, amikor az Országgyűlés elfogadta a Magyar Köztársaság biztonság- és védelem-

¹⁹ TÓTH 2011. 115. o. és 2073/2004. (IV. 15.) Kormány határozat

²⁰ Nbb-13/2001. 10. o.

²¹ SIEBER 2016. 16. o.; FINSZTER 2008. 10. o.

politikájának alapelveit,²² ami kezdőpontjává és alapjává vált a később keletkezett nemzeti biztonsági stratégiáknak.²³ A Magyar Köztársaság biztonság- és védelempolitikájának alapelvei tartalmi részét meghatározza az 1990-es évek hangulata.²⁴ A változást a rendszerváltozást követő években még távolinak tűnő, de mind közelebb kerülő euroatlanti integráció jelentette. Geopolitikai okokból az ország először az Észak-atlanti Szerződés Szervezetéhez, majd az Európai Unió teljes jogú tagságáig került közelebb. Mindezen változások (partváltások²⁵) magukkal hozták a hazánk biztonság- és védelempolitikai és nemzetbiztonsági paradigmaváltását.²⁶ Az ország megfogalmazta a biztonság átfogó értelmezését, az euroatlanti térség biztonságának oszthatatlanságát és stratégiai szintre emelte a biztonság hagyományos politikai és katonai elemein felül a gazdasági, pénzügyi, emberi jogi és kisebbségi, információs és technológiai, környezeti, valamint nemzetközi jogi stb. dimenziókat is.²⁷

A szuperhatalmi szembenállást követően a stratégiai dokumentum lényegesen alacsonyabb valószínűséget tulajdonított a világméretű fegyveres konfliktusoknak, míg a regionális összetűzések lehetősége előtérbe került. A folyamattal párhuzamosan megnőtt az egymás hatását egyidejűleg erősítő új típusú veszélyforrások jelentősége. Az alapelv külön kiemelte az euroatlanti régió biztonságának a fontosságát és a szemlélet hazánk 1999-es NATO, majd 2004-es EU tagsága következtében is meghatározó maradt.²⁸ A növekvő kockázatok sorában első helyen szerepeltek az eltérő társadalmi fejlődésből fakadó, országok és csoportok közötti átmeneti vagy tartós ellentétek, a gazdasági, pénzügyi és társadalmi válságok, az etnikai és vallási feszültségek hatásai. A kiemelt szerepet betöltő kockázati elemek között előtérbe került a terrorizmus, a szervezett bűnözés, az illegális kábítószer- és fegyverkereskedelem, a demográfiai feszültségek, a tömeges migráció és a környezeti ártalmak jelentette kihívások.²⁹ A biztonság- és védelempolitikai alapelvek fokozódó problémaként tekintettek a tömegpusztító fegyverek és azok hordozóeszközeinek elterjedésére, valamint az információs rendszerek sebezhetőségére és utóbbiak elleni támadások lehetséges hatásaira.³⁰ Az 1990-es évek és az ezredforduló tapasztalatai a legnagyobb fenyegetést

²² 94/1998. (XII. 29.) OGY. határozat; valamint azt megelőzően hatályos, a 11/1993. (III. 12.) OGY határozat a Magyar Köztársaság biztonságpolitikai alapelveiről, illetve lásd még a 27/1993. (IV. 23.) OGY. határozat Magyar Köztársaság honvédelmének alapelvei

²³ 2144/2002. (V. 6.) és 2073/2004. (III. 31.) Kormány határozat, majd a napjainkban hatályos 1035/2012. (II. 14.) Korm. határozat

²⁴ KASZNÁR 2017. 98-101. o.

²⁵ Lásd: ADY 1999.

²⁶ IZSA 2003. 76-79. o.

²⁷ 94/1998. (XII. 29.) OGY. határozat 1. pont

²⁸ IZSA 2003. 74. o.

²⁹ Lásd még: KÓHALMI 2015. 52-71. o.

³⁰ HAIG 2007. 37-38. o.

a régió fegyveres kihívásaiban azonosították, miközben hazánk közvetlen környezetében instabilitás és kiszámíthatatlanság jelentkezhett.³¹

A biztonsági problémák regiszterével szemben a Magyar Köztársaság biztonságának alapját az alapelvek két (a gyakorlatban három) pilléren nyugvó építménynek ábrázolta.³² Az egyik, a belső eleme a magyar nemzet önereje; a másik, a külső elem és utóbbi két alrendszere az euroatlanti integráció és a nemzetközi együttműködés³³ tükrözte a szövetségi és közösségi kötelezettségekből eredő elvárásokat.³⁴ A nemzet önereje az integrációs folyamatban is elsődleges maradt az ország biztonságának szavatolásában. A nemzetbiztonsági szolgálatok is ennek a pillérnek a részei,³⁵ még akkor is, ha a Magyar Köztársaság biztonság- és védelempolitikájának alapelvei szövegezésében sehol sem jelent meg a nemzetbiztonsági érdek, a rendvédelmi szervek, vagy a nemzetbiztonsági szolgálatok. A meghatározó nemzeti önerő jellemzése során a jogalkotó a biztonság szavatolása során alapvető fontosságúnak jellemezte az állampolgárok aktív részvételét, támogatását és áldozatkészségét. A stratégia a nemzeti önerőt megtestesítő biztonságpolitika és intézményrendszer működését úgy képzelte el, hogy képes legyen időben felismerni, folyamatosan és megbízhatóan értékelni az ország biztonságát veszélyeztető tényezőket. Az intézményrendszernek információszerző, elemző és értékelő tevékenysége során képessé kellett válni időben meghozni a veszélyhelyzetek megelőzéséhez, illetve elhárításához szükséges döntéseket, valamint végrehajtani az ezekből fakadó intézkedéseket.³⁶

Az általános megfogalmazásnak megvoltak az előnyei és a hátrányai is. Egyfelől, felsorolta a nagyobb figyelmet érdemlő prioritásokat, másrészt megfogalmazta az állami intézményrendszerrel szembeni elvárásokat. Ez utóbbit kellett minden szervezetnek, így a nemzetbiztonsági szolgálatnak is önmagára értelmezni és egy rendkívül fragmentált intézményrendszerben ellátni a jogalkotó által szabott feladatokat. Megvalósítása természetesen nem okozhat problémát, ha rendelkezésre áll a kellően letisztult jogszabályi háttér, konfliktusoktól mentes intézményrendszer, pénzügyi, anyagi és humán erőforrás, valamint a politika-mentes szakmai háttér.

Nemzeti biztonsági és „nemzetbiztonsági” stratégia

A magyar állam biztonság- és védelempolitikai alapelvei határozták meg a magyar állam rendszerváltozást követő biztonsági gondolkodását, ami az ezredfor-

³¹ 94/1998. (XII. 29.) OGY határozat 2. pont

³² 94/1998. (XII. 29.) OGY határozat 6. pont

³³ TÓTH 2011. 116. o.

³⁴ Lásd: NATO 1990., 1991., 1999.

³⁵ IZSA 2009. 11. o.

³⁶ Lásd még: KOVÁCS – DOBÁK 2017. 175-218. o.; 94/1998. (XII. 29.) OGY határozat 9. pont

dulót követően az alapelvek generálklauzuláira épülő nemzeti biztonsági stratégiákban és utóbbiak módosításában öltött testet.³⁷ Az alapelvek és a stratégia tartalmi jelentősége három pontban összegezhető a nemzetbiztonsági szolgálatok nézőpontjából.

Először, a rendszerváltozást követően 1993-ban,³⁸ majd 1998-ban adták ki a magyar biztonsági dokumentumok alapjának tekintett biztonság- és védelempolitikai alapelveket. Az ezredfordulót követően megalkotott első nemzeti biztonsági stratégia szerint a Magyar Köztársaság biztonság- és védelempolitikai alapelveiben megfogalmazott célkitűzéseket elérték és a hazánk biztonságáról alkotott gondolkodást az euroatlanti integráció alapjaiban határozta meg és formálta át.³⁹

Másodszor, a nemzeti biztonsági stratégia lényeges eleme, hogy 2002/2004-től hatályos formában utalást tett a származtatott ágazati stratégiák kidolgozására. A tanulmány témaválasztása és a nemzeti biztonsági stratégia nem-taxatív (példálózó) felsorolásában a nemzetbiztonsági (ágazati) stratégia megalkotásának lehetőségét, szükségességét is megemlíti. A jogalkotó szavai két, egymással összefüggő eredménnyel jártak. Egyfelől semmivel, mert a kormányhatározatban deklarált elhatározásból nem sok minden valósult meg. Másfelől szakmatudományos dialógust indított (nemzetbiztonsági) szakértői körökben és akarva-akaratlanul közös gondolkodásra késztetett a rendvédelmi és nemzetbiztonsági (titkosszolgálati) stratégiáról.⁴⁰

Az elméleti diskurzus egy valós vagy vélt „nemzetbiztonsági stratégia” megalkotásához kívánt hozzájárulni és felölelte a szolgálatok előtt álló kihívásokra, megoldandó feladatokra, az intézményrendszer átalakításának lehetőségeire vonatkozó teoretikus okfejtéseket.⁴¹ Harmadszor, ha az ágazati iránymutatás nem is készült el, a 2002-ben elfogadott, 2004-ben módosított, majd 2012-ben újrafogalmazott nemzeti biztonsági stratégia a legmagasabb szintű dokumentum, ami a jelenleg hatályos formájában már csak deklarálja a hírszerzés és elhárítás fontosságát, de már tartózkodik a hangzatos ígéretektől.⁴²

³⁷ 2144/2002. (V. 6.) Kormány határozat a Magyar Köztársaság új nemzeti biztonsági stratégiájáról, majd 2073/2004. (III. 31.) Kormány határozat a Magyar Köztársaság új nemzeti biztonsági stratégiájáról (módosítás)

³⁸ Lásd: 11/1993. (III. 12.) OGY. határozat a Magyar Köztársaság biztonságpolitikai alapelveiről, valamint a biztonság katonai (honvédelmi) elemére vonatkozó 27/1993. (IV. 23.) OGY. határozat Magyar Köztársaság honvédelmének alapelveiről;

³⁹ 2073/2004. (III. 31.) Kormány határozat; Lásd még: KOVÁCS – DOBÁK 2017. 175-218. o.

⁴⁰ Lásd bővebben: FINSZTER 2008. 2-38. o.; Uő. 2003. 73-81. o.; Uő. 2006. 109-113. o.; TÚTTÓ 2007. 24-36. o.; LÉNÁRT 2001. 41-60. o.

⁴¹ BUDAI 2008. 517-533. o.; LÉNÁRT 2001. 41-60. o.; LAKATOS 2006. 67-74. o.

⁴² 1035/2012. (II. 21.) Kormány határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Magyarország biztonság- és védelempolitikai alapelveinek dokumentuma már a rendszerváltást követő évtizedben megjelölte, a 2002-ben kiadott, 2004-ben módosított, majd 2012-ben új alapokra helyezett nemzeti biztonsági stratégia azonosította a hazánk szempontjából lényeges biztonsági elemeket. A globális kihívások szempontjából vizsgálva, a nemzetbiztonsági szolgálatok feladatkörében súlyponti elemként jelent meg a terrorizmus, a tömegpusztító fegyverek elterjedése, az instabil régiók és működésképtelen államok hatása, az illegális migráció, a gazdasági instabilitás, az információs társadalom kihívásai, illetve a globális természeti, civilizációs és egészségügyi veszélyforrások. Az új évezred belső biztonsági kihívásait a nemzeti biztonsági stratégiában a szervezett bűnözés, a feketegazdaság és korrupció, a kábítószeres terjedése, a politikai és vallási szélsőségek, valamint a demográfiai kihívások jelentették.⁴³ A regionális kihívások között hazánk elhelyezkedése szempontjából Közép- és Délkelet-Európa, a Független Államok Köössége, a mediterrán térség, a Közel- és Közép-Kelet vált hangsúlyossá.⁴⁴

Az ezredfordulót követően a nemzeti biztonsági stratégia alapot kívánt szolgáltatni az államgépezet egészének és ajánlást fogalmazott meg az egymáshoz koherensen kapcsolódó ágazati stratégiák kidolgozásához. A nemzetbiztonsági szolgálatok feladatrendszerre és hangsúlyos területei legkézenfekvőbb módon a nemzeti biztonsági stratégiából kellett, hogy visszatükröződjenek. A dokumentumok általános jelleggel szabtak feladatot az állami intézményrendszer egészének, rajta keresztül az egyes alkotóelemeknek, köztük a szolgálatoknak. Bár a nemzetbiztonsági terület önálló és különálló ágazati stratégiájának kidolgozása elmaradt, nemcsak a származtatott stratégiák, de a rendszerszintű (stratégiai) elképzelés is hiányzott, ami az új évezredben jogos igényként merülhetett volna fel a rendvédelmi szervek és nemzetbiztonsági szolgálatok részéről.⁴⁵ Feltételezhető, hogy a nemzetbiztonsági szolgálatok komplex feladatrendszeréhez kapcsolódó feladatkörök, hatásköri érintkezések az ajánlásban megfogalmazott rendvédelmi, gazdasági-pénzügyi, információvédelmi, vagy a terrorizmus elleni küzdelem területén kidolgozásra ajánlott ágazati stratégiákat összekapcsolhattak volna.⁴⁶ Ha „titkosszolgálati” ágazati stratégiával nem is szolgált a szaktárca, a nemzeti biztonsági stratégia röviden meghatározta, hogy a nemzeti célok elérése érdekében milyen szerepet szán a nemzetbiztonsági területnek.

A kormányzat meghatározása szerint a nemzetbiztonsági szolgálatok a törvényben meghatározott feladataik elvégzésével elősegítették az ország szuverenitásának, alkotmányos rendjének védelmét, nemzetbiztonsági érdekeinek érvé-

⁴³ Resperger 2013. 31-66. o.; Köhalmi 2016. 81-84. o.

⁴⁴ 2073/2004. (IV. 15.) Kormány határozat

⁴⁵ FINSZTER 2008. 33. o.

⁴⁶ 2073/2004 (IV. 15.) Kormány határozat

nyesítését.⁴⁷ A kormányzati döntésekhez szükséges információk biztosításával közvetlenül kellett támogatniuk a döntés-előkészítés folyamatát, valamint gondoskodniuk kellett a megfelelő döntési alternatívák kidolgozásáról, tájékoztatniuk kellett a Kormányt az ország külső és belső veszélyeztetettségének időszerű, illetve távlati alakulásáról. Az információszerzésnek ki kellett terjednie a globális, a regionális és a belső veszélyforrásokra egyaránt. A polgári és katonai nemzetbiztonsági szolgálatoknak feladatuk ellátása során figyelembe kellett venniük a térségünkben bekövetkezett változásokat, az integrációs folyamatokat, az új típusú fenyegetéseket és kihívásokat, a külföldön működő magyar intézményeket, továbbá a válságkezelő és békefenntartó feladatokban részt vevő magyar alakulatokat és szakértőket érintő fenyegetéseket. A nemzetbiztonsági szolgálatok feladatrendszerében kiemelt figyelmet kellett fordítaniuk a határokon átnyúló nemzetközi terrorizmus elleni küzdelemben való részvételre. A Magyarországot érintő biztonsági kihívásoknak megfelelően, valamint az euroatlanti integrációs folyamat sikeres befejezését követően új típusú együttműködést kellett kialakítaniuk és fenntartaniuk a szövetséges államok hírszerző és elhárító szervezeteivel, illetve a nemzeti biztonsági stratégiában megfogalmazott célok elérésében mentén érdekelt más államok szolgálataival.⁴⁸

Főszabályként megállapítható, hogy a nemzetbiztonsági szolgálatok rendszerváltást követő feladatellátásának irányait és hangsúlyait a biztonsági környezetben bekövetkező változások, valamint a hazai és nemzetközi gyakorlat alakította. A jogalkotó csak azt tudja vállalni, hogy az intézményrendszer különböző területeiről származó igényeket rendszerezi, szintetizálja és az egyediből általános célokat fogalmaz meg. A gyakori félreértések és folyamatos elírások miatt ki kell emelni, hogy nemzeti biztonsági stratégia nem egyenlő a nemzetbiztonsági ágazati stratégiával, mely előbbinek egy származtatott ágazati iránymutatása lehetett volna. A biztonság- és védelempolitikai alapelvekre építve a nemzeti biztonsági stratégia az értékek és érdekek mentén meghatározott kereteket alakította ki.

A szakértők a biztonsági környezet értékelésével megfogalmazták az ország adottságából, geopolitikai helyzetéből, a hazánkat érintő biztonságpolitikai kihívásokból származtatott hangsúlyos cél- és feladatcsoportokat, illetve definiálták a nemzeti biztonsági stratégia megvalósításának eszközeit. Feltételezhető, hogy a jogalkotó által készített normatív jellegű, pontos és iránymutató feladatszabás alkalmas lehetett volna arra, hogy belőle a nemzetbiztonsági szféra meghatározza feladatait.⁴⁹

A nemzetbiztonsági szempontból jelentős hangsúlyok tartalmi elemeinek

⁴⁷ Ez az alaptézis jelenik meg az 1995. évi CXCV. törvény 74. §-ban, az Alaptörvény 46. cikkében és az 1035/2012. (II. 21.) 48. pontjában is, amiből minden további feladat származtatott.

⁴⁸ 2073/2004 (IV. 15.) Kormány határozat IV. pont

⁴⁹ IZSA 2007. 20. o.

összekötő elve, hogy a tanulmányban tárgyalt évtizedek dinamikus változásai közepette a nemzetbiztonsági tevékenység célja és lényegi elemei nem változtak. A szervezetrendszer klasszikus funkcionális ágainak elkülönültsége megmaradt, de az elhárítás és hírszerzés közötti határ mind jobban elmosódott, előtérbe került a társ- és partnerszolgálati együttműködés. A mind összetettebb szervezeti és kapcsolati rendszerben a nemzetbiztonsági szolgálatok alaprendeltetése változatlan maradt és előtérbe került, hogy a megváltozott biztonsági környezetben pontos feladatkörrel, stabil jogszabályi keretek között tevékenykedhessenek. Konceptcionálisan a nemzeti biztonsági stratégia a szféra tevékenységét meghatározó titkos információgyűjtési eszközök és módszerek meghatározó jelentőségével, a klasszikus humán források elsődlegességével, valamint az információs- és kommunikációs társadalom előnyeivel és kihívásaival együttesen számolt.⁵⁰ Ez magába kellett, hogy foglalja a rendelkezésre álló informatikai és kommunikációs technika fejlesztését, nagyobb arányú bevonását a rendelkezésre álló információmennyiség feldolgozására, illetve az utóbbival kapcsolatban álló információs biztonság érdekében folytatott tevékenységet.⁵¹

Ha a magyar nemzetbiztonsági stratégia körében következtetéseket kívánunk levonni, akkor tisztában kell lennünk egy lényeges tényállítással: a nemzetbiztonsági stratégia sohasem készült el. Ez utóbbi megállapítás két lényeges tanulsággal és további magyarázatok alapjául szolgálhat. Ez egyrészt mulasztás. Egy mulasztásnak, következetlenségnek mindig van felelőse és jogi, de legalábbis erkölcsi következményekkel kell járnia. Másrészt, a nemzetbiztonsági stratégia nemléte részben igazolta vagy legalábbis feltételezte hiányának lényegtelenességét.⁵² Véleményem szerint a tartós hiány/iránytalanság – amit az új évezred kezdetén már tapasztalni lehetett, már az eredeti kérdést is meg- és maga ellen fordította. A gyakorlatban működőképes nemzetbiztonsági szolgálatoknak nem egy papírra vetett ágazati stratégiára, hanem a formaszerűség mögött meghúzódó tartalomra: egy közép- hosszú távra felépített koncepcióra, az elképzeléshez szükséges forrásokra, utóbbihoz szorosan kapcsolódó következtetességre van és lesz minden időben szükségük.

⁵⁰ SIEBER 2016. 16-18. o.

⁵¹ IZSA 2007. 15-29. o.

⁵² KOVÁCS 2006. 120-122. o.; TÜTTŐ 2007. 27. o.

Összegzés

Összefoglalásként megállapítható, hogy a rendszerváltástól napjainkig a biztonságról alkotott fogalmunk és gondolkodásunk alapjaiban változott meg és alakult át. Nincsen egy állandó és kiszámítható fejlődési ív, általános szabályok, nem lehet minden lehetséges biztonsági kockázatra felkészülni és minden forgatókönyvet számba venni. A nemzeti biztonsági stratégia célja, hogy regiszter és sorvezető legyen, összefoglalja az állam biztonságát veszélyeztető elemeket. Az elmúlt évtizedek változásai feloldották a külső és a belső biztonság, az állam és a magánszektor, a prevenció és a represszió, valamint az ezekhez korábban egyenként hozzárendelhető, elkülönült eszközöket és szervezeteket. Nincsen élesen szétválasztható szervezetrendszer és hozzárendelt feladat, ahogy önmagában kezelhető biztonsági probléma sem létezik.

A nemzetbiztonsági szolgálatok feladatellátásának hangsúlyait és kereteit a nemzeti biztonsági stratégia – mint egy széles értelemben vett regiszter – és a vonatkozó jogszabályi háttér kijelölte. Látszólag pontosabb meghatározást a gyakorlat az elmélettől nem igényelt. A gondolat egy részről jogos, elvégre fel kell ismerni, hogy a biztonságpolitikai hangsúlyok és veszélyforrások univerzálisak. A biztonsági kockázatok közül nem lehetett kiragadni egyet sem, aminek csak és kizárólag nemzetbiztonsági/titkosszolgálati aspektusa lenne, vagy önmagában ne kapcsolódna további biztonsági területekhez. Hivatkozott biztonsági halmazból származtatott feladatok mindegyikére igaz, hogy ellátásuk komplex tevékenység. Ez a feladatellátás minden esetben társzolgálatok, további rendvédelmi szervezetek bevonását igényli, ahol az egyes hatáskörök jogalkotói elhatárolása sem könnyű feladat. A 2002-ben kiadott, majd 2004-ben módosított és 2012-ben új alapokra helyezett nemzeti biztonsági stratégia kategorizálta a Magyar Köztársaság, később Magyarország biztonságát fenyegető veszélyeket és kihívásokat, ahol a komplex feladatellátás részeként a nemzetbiztonsági szféra ellátta a különleges rendeltetéséből adó nyílt vagy titkos információgyűjtő tevékenységet, az egyes veszélyek horizontális felderítését, előre jelzését és megelőzését. A kormányzat által 2012-ben kiadott új nemzeti biztonsági stratégia a módosított elődjétől eltérően, terjedelmesebben vette számba hazánk védendő értékeit és érdekeit, elemezte az ezredfordulót követően átalakult biztonsági környezetet és Magyarország nemzeti biztonsági érdekeit a nemzeti célok és feladatok, valamint kormányzati eszközök pontosabb megjelölésével kívánja biztosítani

Felhasznált irodalom:

- 1035/2012. (II. 21.) Kormány határozat Magyarország Nemzeti Biztonsági Stratégiájáról;
- 11/1993. (III. 12.) OGy határozat a Magyar Köztársaság biztonságpolitikai alapelveiről;
- 1990. évi X. törvény a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról;
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról;
- 2073/2004. (III. 31.) Kormány határozat a Magyar Köztársaság új nemzeti biztonsági stratégiájáról (módosítás);
- 2144/2002. (V. 6.) Kormány határozat a Magyar Köztársaság új nemzeti biztonsági stratégiájáról;
- 26/1990. (II. 14.) Minisztertanácsi rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról;
- 27/1993. (IV. 23.) OGy. határozat Magyar Köztársaság honvédelmének alapelveiről;
- 94/1998. (XII. 29.) Országgyűlési határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről;
- Magyarország Alaptörvénye;
- NATO [1991] The Alliance's New Strategic Concept
http://www.nato.int/cps/en/natolive/official_texts_23847.htm (2016. január 10.);
- NATO [1995] Study on NATO Enlargement
http://www.nato.int/cps/en/natolive/official_texts_24733.htm (2016. január 10.);
- NATO [1999] The Alliance's Strategic Concept
http://www.nato.int/cps/en/natolive/official_texts_27433.htm (2016. január 10.);
- NATO [2010] Active Engagement, Modern Defence
http://www.nato.int/cps/en/natolive/official_texts_68580.htm (2016. január 10.);
- Országgyűlés Nemzetbiztonsági Bizottsága nyilvános üléseinek jegyzőkönyvei;
- Ady Endre: Ismeretlen Korvin-Kódex margójára. In: Szabolcsi József (szerk.): Ady Endre összes művei. Arcanum Adatbázis Kft., Budapest, 1999.;
- BODA József: A felderítés, hírszerzés, titkos információgyűjtés elvei és gyakorlata. Belügyi szemle 2015/9. 5-29. o.;
- DEZSŐ Lajos, HAJAS Gábor: A nemzetbiztonságra vonatkozó jogszabályok. HVG-ORAC, Budapest, 1998.;

- FINSZTER Géza: A nemzetbiztonságról. Rendészeti Szemle, 1991/1. 5-17. o.;
- FINSZTER Géza: Ismét a nemzetbiztonságról. Belügyi Szemle, 1999/4-5. 5-19. o.;
- GÁL István: A nemzetközi kötelezettségen alapuló közbiztonsági célú gazdasági előírások elleni bűncselekmények. In: Polt Péter (szerk.): Új Btk. Kommentár. 6. kötet. Nemzeti Közszerológálati és Tankönyvkiadó Zrt., Budapest, 2014. 53-74. o.;
- GAZDAG Ferenc (szerk.): Biztonságpolitika. SVKH, Budapest, 2001.;
- HAIG Zsolt: Az információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány, 2007/3. 37-56. o.;
- HANS-JÖRG, Albrecht: A biztonságkonceptió átalakulása és ennek következményei az európai bel- és jogpolitikára. Belügyi Szemle, 2006/2. 3-26. o.;
- HAUZINGER Zoltán: A fegyveres szervek rendeltetésének alaptörvényi szabályozása. In: Drinóczi Tímea (szerk.): Magyarország új alkotmányossága. PTE ÁJK, Pécs, 2011. 65-76. o.;
- IZSA Jenő: A titkosszerológálati/nemzetbiztonsági ágazati stratégiáról. Hadtudomány, 2006/4. 109-113. o.;
- IZSA Jenő: A titkosszerológálati/nemzetbiztonsági ágazati stratégiáról. Hadtudomány, 2006/4. 109-113. o.;
- IZSA Jenő: A titkosszerológálatok tevékenységének általános jellemzői, ellenőrzésük és irányításuk kérdései. Szakmai Szemle (Katonai Biztonsági Hivatal), 2009/2. 5-19. o.;
- IZSA Jenő: Az ország biztonságát és a védelmi szféra helyzetét befolyásoló körülmények, tényezők. Szakmai Tudományos Közlemények (Katonai Biztonsági Hivatal Tudományos Kutatóhely és Magyar Honvédség Térképész Szerológálat) 2003 73-81. o.;
- IZSA Jenő: Javaslatok a nemzetbiztonsági/titkosszerológálati stratégia kidolgozásához. Hadtudomány, 2007/1. 15-29. o.;
- IZSA Jenő: Nemzetbiztonsági alapismeretek. A titkosszerológálatok működése. ZMNE, Budapest, 2009.;
- KASZNÁR Attila: A terrorizmus megjelenése Magyarországon az 1970-es és 1980-as években. (T)error & Elhárítás 2017/1-2. 98-101. o.;
- KOVÁCS Vendel: A titkosszerológálatok „természetrájza”. Rendészeti Szemle, 1994/12. 14-17. o.;
- KOVÁCS Zoltán Andás - DOBÁK Imre: Korszakváltások a magyar nemzetbiztonsági intézményrendszerben. In: Finszter Géza – Sabjanics István (szerk.): Biztonsági kihívások a 21. században. Dialóg Campus Kiadó, Budapest, 2017. 175-218. o.
- KŐHALMI László: A migráció néhány biztonságpolitikai összefüggése. Szakmai Szemle 2016/4. 81-100. o.;
- KŐHALMI László: Gondolatok a vallási indíttatású terrorizmus ürügyén.

Belügyi szemle 2015/7-8. 52-71. o.;

- LÉNÁRT Ferenc: Biztonság, nemzetbiztonság. Új Honvédségi Szemle, 2000/1. 41-59. o.;
- MATUS János: A nemzeti és nemzetközi biztonság változása a globalizáció hatására. Szakmai Szemle (Katonai Nemzetbiztonsági Szolgálat), 2012/1. 55-63. o.;
- RESPERGER István: Biztonsági kihívások, kockázatok és fenyegetések 2030-ig. In: Kobolka István (szerk.): Nemzetbiztonsági alapismeretek. Nemzeti Közzolgálati és Tankönyvkiadó Zrt. Budapest, 2013. 31-66. o.;
- RÉVÉSZ Béla: Az állambiztonságtól a nemzetvédelemig. SZTE ÁJK, Szeged, 2003.;
- SIEBER Ulrich: The paradigm shift in the global risk society: from criminal law – an analysis of the changing limits of crime control. Journal of Eastern European Criminal Law 2016/1. 14-27. o.;
- TÓTH Csaba Mihály: Az együttműködés, mint az új kihívások hatására fokozódó követelmény a nemzetbiztonsági szférában. Szakmai Szemle 2011/3. 114-122. o.;
- TÜTTŐ Szabolcs: A nemzetbiztonsági szolgálatok feladatrendszere az új kihívások tükrében. Hadtudomány, 2007/3. 24-36. o.;

Rivalizáció a kádári hírszerzésben

Gyömbér Béla¹

Absztrakt:

A rendszerváltozás előtt két szervezet, a BM III./I. és az MNVK-2 látta el a hírszerzés feladatait. A két intézmény méretben és szakmaiságban is jelentősen eltért egymástól. A BM III. szinte minden területen jelen volt, míg az MNVK-2 jóval specializáltabban működött. Mivel a tevékenységeik részben fedték egymást, ezért az együttműködés alapvető fontosságú lett volna. Erről egyébként parancs és további utasítások is rendelkeztek. A valóságban azonban előfordult, hogy a rivalizálás olyan méretű vált, hogy a BM büntetőeljárást indított az MNVK-2 fedett tevékenysége ellen.

Kulcsszavak: MNVK-2, BM III., Metalimpex

Abstract:

Before the change of regime two organizations, the BM III./I. and the MNVK-2 carried out the tasks of intelligence. The two institutions were differed greatly in size and professionalism. The BM III. was present in almost every area, while the MNVK-2 functioned much more specially. As their activities partially covered each other, therefore their cooperation would have been essential. About this topic they even initiated commands and instructions. But in reality the rivalry was such serious that BM initiated criminal proceedings against MNVK-2's covered activities.

Keywords: MNVK-2, BM III., Metalimpex

¹ ORCID azonosító: orcid.org/0000-0002-5634-7463

Bevezetés

A rendszerváltozás előtti magyar titkosszolgálatok működéséről egyre több információ kerül feldolgozásra. Ebbe a sorba illeszkedik Dr. Borvendég Zsuzsanna doktori munkája, amely az „Újságírók és külkereskedők a Kádár-rendszer hírszerzésében” címet kapta.

A jelen cikkben többször is idézett doktori értekezés² nem kizárólag a rendszerváltozás előtti újságírást vette speciális górcső alá, hanem a Kádár-korszak alatt létrehozott, sajátos, külföldi elemekre is támaszkodó, offshore jellegű céghálózat elemeit is bemutatja, amelyek irányításáért a korabeli titkosszolgálatok versenyben álltak egymással.

A tanulmányának bizonyos fejezeteiből egyértelműen kitűnik a Belügyminisztérium III. Főcsoportfőnöksége, mint a legnagyobb hazai hírszerző szolgálat és egy jóval kisebb, a hazai közvélemény előtt talán jóval szűkebb körben ismert szervezet, a Magyar Néphadsereg Vezérkara 2. Csoportfőnökség közötti rivalizáció.

Első ránézésre elmondható, hogy a két szervezet között igen jelentősek voltak a méretbeli eltérések. Tulajdonképpen szorosan a katonai jellegű adatokra vonatkozó hírszerzést kivéve minden más titkosszolgálati feladatot a Belügyminisztérium III. Főcsoportfőnöksége (BM) látott el, „még a hadseregen belüli elhárítás is hozzájuk tartozott, sőt, a hetvenes-nyolcvanas évek fordulójától NATO-ellenes hírszerzést is folytattak.”³ Ezzel szemben a Magyar Néphadsereg Vezérkara 2. Csoportfőnöksége (MNVK-2) jóval szűkebb erőforrásokra támaszkodhatott és a tevékenységi köre is behatároltabb volt.

Dr. Hajma Lajos „A katonai felderítés és hírszerzés története” című egyetemi jegyzetében arról írt,⁴ hogy az MNVK-2 felsőbb szintű állami szabályozás alapján alapvetően együttműködött a III/I-es, valamint a külföldön szolgáló katonadiplomácia vonatkozásában a III/II-es Csoportfőnökségek illetékes szakembereivel.

A III. Főcsoportfőnökség megjelölésére a továbbiakban egységesen a BM megjelölést is használok az egymással nyilvánvalóan szorosan együttműködő III/I. és III/II. Csoportfőnökségekre tekintettel. Mára ennek az együttműködésnek

² BORVENDÉG Zsuzsanna: *Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016.,* <http://real-phd.mtak.hu/456/1/Borvend%C3%A9gZsuzsanna.pdf> (Megtekintés: 2017.08.15)

³ BORVENDÉG Zsuzsanna: *Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016., 158. old.* <http://real-phd.mtak.hu/456/1/Borvend%C3%A9gZsuzsanna.pdf> (Megtekintés: 2017.08.15)

⁴ Dr. HAJMA Lajos: *A katonai felderítés és hírszerzés története, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2001, 163. old.*

a jogi keretei is megismerhetővé váltak. Egyáltalán nem volt tehát szükségszerű a kifejezett rivalizáció, sőt, inkább együttműködő intézményeknek kellett volna lenniük, amire egyébként külön parancs is kötelezte a szervezeteket, amit a későbbiekben részletezni fogok majd.

Dr. Borvendég Zsuzsanna értekezése egyébként azt is sejtetni engedi, hogy a két szervezet közötti versengés korántsem biztos, hogy szakmai alapú volt: szerte a rendszer mélyén ugyanis egyéni érdekek mentén is zajlott a kapitalizmus káros elemeinek, mint a szervezett bűnözés és a korrupció átemelése.

A két szervezett közötti együttműködésről számos olyan dokumentum vált megismerhetővé, melyek betekintést engednek abba a jogszabályi környezetbe, amelynek keretei között dolgozniuk kellett volna. Az Állambiztonsági Szolgálatok Történeti Levéltára (ÁBTL) által üzemeltetett weboldalon⁵ ugyanis elérhetővé váltak a korábban még minősítés alatt álló, a témakörre vonatkozó parancsok és utasítások is.

Dr. Borvendég Zsuzsanna a BM és az MNVK-2 állománya közötti különbségeket egyébként úgy jellemzi, hogy az MNVK-2 állományon kívüli embereinek többségét nem is ügynökként, hanem „megnyertként” tartották számon, amely kapcsolat kevésbé volt formalizált.⁶ Ezt alátámasztja Nagy Gyula „A magyar katonai képzések története (1945 – 1990)” c. tanulmánya is, miszerint valóban nem volt különösebben hosszú a kiképzés az MNVK-2 állományában.⁷

Más források alapján az MNVK-2 tevékenysége lehet, hogy specializált volt, de azon a területen meglehetősen önállóan tevékenykedhetett. A vezetője például közvetlenül a vezérkari főnök egyik (felderítő) helyettese volt. Magyar Balázs tanulmánya⁸ szerint az MNVK-2 '80-as években működő szervezete már nagyon is hatékonyan integrálta a hadászati, a hadműveleti-harcászati és a harcászati felderítési szinteket.

A BM-hez képest szűkös erőforrások is szerepet játszhattak abban, hogy az MNVK-2 végül illegális erőforrásokat is bevont a működésének a finanszírozásába. Mint arról a tanulmány részletesen beszámol: a közvetve az MNVK-2 által

⁵ <http://www.abparancsok.hu/>

⁶ BORVENDÉG Zsuzsanna: Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016., 99. old. <http://real-phd.mtak.hu/456/1/Borvend%C3%A9gZsuzsanna.pdf> (Megtekintés: 2017.08.15)

⁷ NAGY Gyula: A magyar katonai képzések története (1945 – 1990), Nemzetbiztonsági Szemle, 2014. Különszám I., 59. old., http://epa.oszk.hu/02500/02538/00004/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_01kszo_058-067.pdf (Megtekintés: 2017.08.15)

⁸ MAGYAR Balázs: A magyar katonai hírszerzés tevékenységének fő irányai és jellemzői a versói szerződés időszakában, Hadtudományi Szemle 2008/2. http://epa.oszk.hu/02400/02463/00002/pdf/EPA02463_hadtudomanyi_szemle_2008_2_014-021.pdf (Megtekintés: 2017.08.15)

irányított Metalimpex elnevezésű vállalat olyan szinten illegálisan működött, hogy a BM 1974 végén végül tudatosan bűnügyi nyomozást indított a vele érvényes parancs alapján egyébként együttműködni köteles másik hazai szolgálat fedett tevékenysége ellen.

Titkos parancsok

Mielőtt azonban a rivalizálásra utaló, konkrét esetet bemutatnám, szeretnék kitérni arra is, hogy 1974-ben, illetve azt megelőzően milyen jellegű együttműködést írtak elő a szervezetek működésére vonatkozó, hatályban levő parancsok és utasítások. Az egyik ilyen szabályozó a Magyar Népköztársaság Honvédelmi Miniszterének és Belügyminiszterének 002. számú parancsa volt, amelyet 1964. július 30-án adtak ki.⁹

A parancs szövege alapján úgy tűnik számomra, hogy a BM és az MNVK-2 közötti együttműködés már akkoriban sem volt zökkenőmentes, bár azt írták, hogy „az eddigi együttműködés a felmerült hiányosságok ellenére egészében véve eredményes volt.”¹⁰ A külön parancs megalkotásának hivatalos indoka tehát nem az volt, hogy problémák lennének az együttműködéssel, hanem az, hogy annak szintjét – a parancs segítségével – „magasabb szintre” emeljék.

Általánosságban elmondható, hogy mindkét szervezetnek széleskörű tájékoztatási kötelezettsége volt a másik felé, illetve operatív együttműködésre vonatkozó szabályok is előírásra kerültek már 1964-ben is, amelyek főként a beszerzések lebonyolítását érintették. A témakör szempontjából elsődlegesen az MNVK-2 BM részére nyújtandó tájékoztatási kötelezettségére vonatkozó szabályok a legfontosabbak, ezért azokat ismertetném részletesebben.

A Magyar Néphadsereg Vezérkari Főnökének 43. számú utasítása alapján¹¹ az MNVK-2 folyamatosan és időben volt köteles tájékoztatni a BM. III/I. Csoportfőnökséget a feladataival összefüggő értesüléseikről és a Magyar Népköztársaság külképviseletei és a külképviseletek fedése alatt működő rezidentúrák biztonsági helyzetét érintő problémákról is.

Tájékoztatási kötelezettsége volt továbbá a célterületet képező kapitalista országokban kialakult operatív helyzetről és ennek változásairól, valamint a biztonsági, közigazgatási és egyéb szervek ellenőrző tevékenységéről és módszereiről.

⁹ A Magyar Népköztársaság Honvédelmi Miniszterének és Belügyminiszterének 002. számú parancsa, Budapest, 1964. július 30.,

http://www.abparancsok.hu/sites/default/files/parancsok/10_27_2_1964.pdf (Megtekintés: 2017.08.15)

¹⁰ *uo.* 1. old.

¹¹ A Magyar Néphadsereg Vezérkari Főnökének 43. számú utasítása, Budapest, 1964. július 30., 1. old.,

http://www.abparancsok.hu/sites/default/files/parancsok/10_27_2_1964.pdf (Megtekintés: 2017.08.15)

ről, valamint az MNVK-2 által tervezett olyan jelentősebb akciókról is, amelyek az ellenséges szervek ellenőrző és korlátozó tevékenységének fokozását, vagy ellenintézkedéseit vonhatták maguk után.

Emellett együttműködési kötelezettségük volt a beszerzési jelöltek felkutatására, kiválasztására és tanulmányozására irányuló munkában, valamint a külképviseletek biztonsága és védelme terén is. Egymás erőforrásait is felhasználhatták, amennyiben az nem zavarta a másik szervezet tevékenységét.

A Magyar Néphadsereg Vezérkari Főnökének 44. számú utasítása rendelkezett a BM. III/II. Csoportfőnökséggel való együttműködésről, melynek során az MNVK-2 rendszeresen tájékoztatni volt köteles a BM. III/II-t a megadott hírigény alapján szerzett értesülésekről, az ellenséges hírszerző és elhárító szervek tevékenységében értékelésük szerint bekövetkezett változásokról, a kapitalista országok Magyarországon tevékenykedett katonai attaséiról, személyi kéréseikről.¹²

Dr. Borvendég Zsuzsanna a doktori értekezésében egyébként gyakran használja az „illegális tevékenység” kifejezést.¹³ Bármilyen meglepő: ez a vizsgált területen valóban nem volt szokatlan, sőt, nemhogy nem volt szokatlan, hanem egyenesen a munkamódszer egyik fajtáját jelentette az illegális tevékenység.

A már említett parancs például úgy rendelkezik, hogy „mindazokat a legális, vagy illegális úton szerzett értesüléseket és adatokat, amelyek a másik szerv ügyrendben meghatározott feladatkörével függnek össze, vagy munkájának megszervezését, operatív biztonságának fenntartását és fokozását (operatív helyzettel kapcsolatos ismeretek) segíthetik elő, időben adják át egymásnak.”¹⁴

A parancsból, illetve utasításokból azonban furcsa módon meglehetősen kevés konkrétum került át a BM III. Főcsoportfőnökség 1967-es ügyrendjébe.¹⁵ A III/I. Csoportfőnökség köteles volt ellátni az MNVK-2-t a titkos operatív és hír-

¹² A Magyar Néphadsereg Vezérkari Főnökének 45. számú utasítása Budapest, 1964. július 30., 1. old.,

http://www.abparancsok.hu/sites/default/files/parancsok/10_27_2_1964.pdf (Megtekintés: 2017.08.15)

¹³ Például Borvendég Zsuzsanna: Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016., 58. old. <http://real-phd.mtak.hu/456/1/Borvend%C3%A9gZsuzsanna.pdf> (Megtekintés: 2017.08.15)

¹⁴ A Magyar Népköztársaság Honvédelmi Miniszterének és Belügyminiszterének 002. számú parancsa, Budapest, 1964. július 30., 1. old..

http://www.abparancsok.hu/sites/default/files/parancsok/10_27_2_1964.pdf (Megtekintés: 2017.08.15)

¹⁵ A BM III. Főcsoportfőnökség ügyrendje, Budapest, 1967,

http://www.abparancsok.hu/sites/default/files/parancsok/10_1837_1967.pdf (Megtekintés: 2017.08.15)

adástechnikai, valamint biztonsági eszközökkel,¹⁶ a III/3. Osztály feladatul kapta az MNVK-2 részéről igényelt operatív feladatok teljesítését,¹⁷ a III/I. Csoportfőnökség pedig szoros együttműködésre volt köteles az MNVK-2-vel,¹⁸ azonban annak módjának különösebb részletezése nélkül.

A Belügyminisztérium III. Főcsoportfőnökség 1972-es ügyrendje pedig már csak annyit tartalmazott, hogy a BM. III/V. Csoportfőnökség feladata biztosítani az operatív technikai eszközöket az MNVK-2 feladatainak elvégzéséhez.¹⁹

A Magyar Népköztársaság belügyminiszterének 009. számú, 1973. június 12-én kelt utasítása viszont kiterjesztette a már bemutatott 002/1964. számú parancsot a rendőr-főkapitányságok szerveire is. Az érintett szervek vezetőinek a hálózati és egyéb operatív úton megszerzett, vagy tudomásukra jutott katonai és katonapolitikai jellegű adatokat és információkat ezentúl rendszeresen az MNVK Felderítő Csoportfőnökség rendelkezésére kellett bocsátaniuk. Érdekesség, hogy az információt tartalmazó jelentéseken — a forrás megjelölése nélkül — fel kellett tüntetni a megbízhatóság és ellenőrzöttség fokát is.²⁰

Az ügynöki munkán kívül, az operatív munka más területein a rendelkezésre álló egyéb operatív eszközök (vizsgálat, operatív nyilvántartás, környezettanulmány, külső figyelés stb.) felhasználásában is — a konspiráció szigorú szem előtt tartásával — pedig „jó együttműködést” kellett megvalósítani.²¹

A „papíron” tehát széles körű együttműködésben azonban a gyakorlatban komoly problémák merültek fel, amelynek eredményeként az egyik esetben például a BM büntetőeljárást kezdeményezett az MNVK-2 „megnyertjei” ellen, akik nem mellesleg az egyik legfontosabb állami külkereskedelmi céget, a Metalimpexet irányították.

Metalimpex

A rivalizálásra példaként most bemutatásra kerülő büntetőeljárásra utaló információk többféle forrásból is elérhetők. Egy, a Hadtörténeti Intézet és Múzeum-

¹⁶ *uo.* 18. old.

¹⁷ *uo.* 25. old.

¹⁸ *uo.* 29. old.

¹⁹ *A Belügyminisztérium III. Főcsoportfőnökség ügyrendje, Budapest, 1972, 18. old.*
http://www.abparancsok.hu/sites/default/files/parancsok/10-530_1972.pdf (Megtekintés: 2017.08.15)

²⁰ *A Magyar Népköztársaság belügyminiszterének 009. számú utasítása, Budapest, 1973., 3. old.*
http://www.abparancsok.hu/sites/default/files/parancsok/10_22_9_1973.pdf (Megtekintés: 2017.08.15)

²¹ *uo.* 4. old.

hoz köthető kimutatás szerint²² például az 1815-ös doboz 3525-ös őrzési egység az MNVK Titkárságától 0,010 ifm mennyiségű adatot tartalmazott.

Ez az iratanyag tartalmazta a „METALIMPEX külkereskedelmi vállalat büntetőeljárással alá vont vezetőivel kapcsolatban 1974.” elnevezésű jelentést és az „MNVK 2. Csoportfőnökség munkájának ellenőrzésére, és jelentés ennek végrehajtásáról 1975.” szóló vizsgálati tervet is. Talán nem véletlenül egy egységben kezelve ezt a két iratanyagot.

A vizsgálati tervre nyomós persze okot adhatott, hogy a BM számára világossá vált: legalább 1970-től kezdve a Metalimpex két, az MNVK-2 által „beszervezett” vezetője, Gergely Miklós és Dévai István is „valutakitermelést” folytatott a katonai titkosszolgálat számára. Az MNVK-2 pedig – talán meglepő módon – azonnal mögéjük állt, és igazolták, hogy a „megnyertjeik” nem a saját hasznukra követik el a gazdasági visszaéléseket, vagyis bíróság előtt tetteikért nem lehet őket felelősségre vonni. A BM azonban nem így gondolta.

Gergely Miklós személye jól példázza az MNVK-2 által „megnyertek” körét. A korabeli sajtóban, szakfolyóiratokban megismerhető nyilatkozatai alapján személyisége némileg különbözött a sztereotipikus kommunista vállalatvezetéstől. A korabeli sajtóban bírálta a legalapvetőbb közgazdaságtani elveket is semmibe vevő, szakmaiatlan tervgazdálkodást és a silány minőségű tömegtermelést.²³

A katonai felderítés egyébként később azt állította, hogy Dévai 1970-ben ajánlotta fel a „valutakitermelésre” vonatkozó szolgálatait tartótisztjeinek, de mivel 1958-tól folyamatosan kapcsolatban állt a katonai titkosszolgálattal, ezért elképzelhető, hogy az általa végzett „valutakitermelés” is korábban kezdődött.²⁴

Médiaajelenlét

A témakör más forrásból történő megismeréséhez felkutattam a korabeli cikkeket, amelyek a Metalimpex vállalattal, illetve annak vezetésével voltak kapcsolatosak. A külkereskedelmi vállalat sajtómegjelenése alapján már 1965-66-ban – vagy talán még korábban – körvonalazódhatott a későbbi „valutakitermelés” koncepciója. A korabeli sajtóinformációkat azonban nyilvánvalóan fenntartással kell kezelni, hiszen az MNVK-2 komoly befolyással bírt ezen a területen is.

Gergely Miklós 1965-ben azzal került a Külkereskedelem c. szaklap interjúalanyai közé, hogy a munkája nyomán a Metalimpex nyerte el a Minisztertanács

²² <http://www.militaria.hu/adatb/leveltariuj/sites/default/files/MN1979%20I..DOC> (Megtekintés: 2017.08.15)

²³ Például: Külkereskedelem, 1963/12., A vállalatok közgazdasági munkájáról (Jakabfi István)

²⁴ BORVENDÉG Zsuzsanna: Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016., 108. old. <http://real-phd.mtak.hu/456/1/Borvend%C3%A9gZsuzsanna.pdf> (Megtekintés: 2017.08.15)

és a SZOT vörös vándorzászlaját.²⁵ 1964-ben a Metalimpex már az egész magyar külkereskedelem 12 százalékát bonyolította, és az első nagyobb exportsikerek is ekkor kezdődtek. Mindazonáltal vállalat életében a '60-as évek második feléig így is az import és esetlegesen a szocialista országokba történő export dominált.

A Nógrád című lap 1966. március 13-i számában Dévai már azt szorgalmazta,²⁶ hogy devizakeretet biztosítsanak annak érdekében, hogy a jövőben többen jussanak ki külföldre, „tapasztalatcserére,” az Acélgyár szakemberei közül is. A külföldi kapcsolatépítéshez ugyanis rugalmas utazási lehetőségekre volt szükség, ami a korabeli körülmények között egyáltalán nem volt evidens.

1970 környékére már viszonylag szabadon mozoghattak a külkereskedelemmel foglalkozó vállalatok képviselői külföldön, azonban 1971-ben szigorítást vezetett be a kormány, noha az „impex” (a különböző „impex” vállalatok hálózata alapján feltételezhető, hogy legalább részben, vagy egészben hasonló célokat szolgáltak, mint a Metalimpex) gyárigazgatók határozottan kijelentették: a piaci követelményekhez való gyorsabb igazodásban, a tempósabb gyártás és gyártmányfejlesztésben nagy része van a külföldön járt gyári szakembereknek.

A Nógrád 1971. február 25-i számában a külföldi exportban érdekelt hazai vállalatok vezetőinek találkozájáról készül egy egész oldalas beszámoló.²⁷ A szigorítást ellenző véleményekre reagálva Hegedűs János, a Külkereskedelmi Minisztérium pártbizottságának titkára jelezte, hogy a kormány számtalan esetben meggyőződött, de „a mi külkereskedelmi vállalataink vezetői is gyakran elmondták, hogy olyanok is utaznak külföldre, akiknek semmi keresnivalójuk ott.”²⁸

A párt legfelsőbb szintjén is akadhattak tehát olyanok, akiknek nem tetszett a nagyfokú szabadság és talán a leplezett tevékenységről is tudomást szerezhettek. Nagyon hiányzik az eddig megjelent tanulmányokból a Metalimpex és az MNVK-2 történetének belehelyezése az új gazdasági mechanizmus rendszerébe, amelynek kialakítása ugyanekkor zajlott.

A reformokat ígérő gazdasági rendszert ugyanis 1960-as évek közepén készítették elő, és 1968. január 1-jén vezették be. Akár üzenetként is fel lehet fogni a Nógrád 1970. szeptember 10-i számában megjelent cikket az acélipari termékek exportja kapcsán, ami azt a címet kapta, hogy „A pártkongresszus tiszteletére a túlteljesítés is kevés...”²⁹

A Metalimpex pénzügyi helyzetét elemezve elmondható, hogy a Világgazdaság 1969. februári számában Dévai István már elképesztő exportbővülésről szá-

²⁵ *Külkereskedelem, 1965/6., 3 kérdés – 3 felelet (Interjú Gergely Miklóssal, a Metalimpex igazgatójával)*

²⁶ *Nógrád, 1966. március 13.*

²⁷ *Nógrád, 1971. február 25., Megtálták az együttműködés új, eredményes formáit, 5. old.*

²⁸ *uo.*

²⁹ *Nógrád, 1970. szeptember 10., A pártkongresszus tiszteletére a túlteljesítés is kevés..., 1. old.*

molt be.³⁰ Az előző évi adatokat elemezve kiderül, hogy a tőkés export (nem szocialista országok felé irányuló export) az előző évben 47 százalékkal nőtt. Az eredményeket az új gazdasági mechanizmus működésével magyarázta. A lap 1969. decemberi száma alapján azonban úgy tűnik, hogy a „jó konjunktúra” ellenére is úgy döntöttek,³¹ hogy az előző évinél kevesebb nyereségrészesedést fizetnek a dolgozóknak, mint egy évvel korábban.

A Világgazdaság 1970 áprilisi számában ennek ellenére is kiemelkedően sikeresnek ítélte az 1969-es évet Gergely Miklós.³² Míg a tőkés export 1968-ban 1,9 százalékkal, 1969-ben már 44 százalékkal múlta felül az importot. A Metalimpex ezeken az éveken jelentősen átalakította a népgazdaságban elfoglalt helyét, mivel korábban a forgalma főleg importból származott.

A Metalimpex és egyébként az egész „impex” céghálózat önmagában is (vagyis a „valutakitermelés” és más illegális, illetve szürkezónás tevékenységek mellett) alapvető fontosságú lehetett a katonai hírszerzés számára, hiszen szinte az egyetlen lehetőséget jelentette arra, hogy nagyobb számú magyar állampolgár nyugatra távozhasson és ott felderítő tevékenységet folytasson.

A pénz beszél, a valuta kitermelődik

De miről is szólt a „valutakitermelés” és ezzel összefüggésben a Metalimpex üzletelése? Lényegében a katonai hírszerzés bázisaként működött. „A Kádár-rendszer idején ugyanis nemritkán titkosszolgálati segítséggel történt pénzkivonás az állami vállalatokból, a titkosszolgálatok pedig igyekeztek minél nagyobb szeletet kiszakítani az államilag monopolizált piacokból.”³³

Az MNVK-2 Csoportfőnökség költségvetési keretének kiegészítésére már az ötvenes évek második felétől felhasználta a Metalimpex Külkereskedelmi Vállalatot – korabeli operatív szóhasználatul élve: „bázisszervként” tekintett rá. A pénzkivonás egyik legegyszerűbb módja a különböző közvetítők, vagyis kereskedelmi ügynökök közbeiktatása volt.

„Ez egészen egyszerűen azt jelentette, hogy magyar részről nem közvetlenül a partner céget kereste meg vételi vagy eladási szándékával a vállalat, hanem egy meghatározott üzletkötőt bízott meg az ügylet lebonyolításával.”³⁴ Az ilyen üzletkötők persze ténylegesen is segíthették egy-egy ügylet lebonyolítását. Azonban az eljárásukért kifizetett összegek gyakran messze meghaladták az elévült, vagy a néha talán nem is létező munkájuk valódi értékét.

Az illegális tevékenységbe bevont közvetítők tehát a tevékenységükért magas jutalékokat kaptak, és ezekből meghatározott százalékot visszaszolgáltattak,

³⁰ *Világgazdaság*, 1969. február 7., *Gondok és eredmények a Metalimpexnél*

³¹ *Világgazdaság*, 1969. december 2., *Hozzászólás a nyereséghez*

³² *Világgazdaság*, 1970. április 29., *A világpiacon árk hatása a METALIMPEX-re*

³³ *uo.* 87. old.

³⁴ *uo.* 109. old.

a Metalimpex esetében Dévai Istvánnak, aki a pénzt továbbította az MNVK-2 részére. Ez a pénzáramlás általában a központi bankon keresztül zajlott, de a Metalimpex esetében az MNB nem kapott szerepet, Dévai István pedig a központi bank megkerülésével szervezte az illegális pénzek eljuttatását a titkosszolgálatokhoz.³⁵

A közvetítőkön alapuló bonyolult cégháló természetesen operatív célokat is szolgált, hiszen az USD alapon befutó jutalékok fedett összegek voltak, amit a Szovjetunió és a keleti blokk országai felhasználhattak a külföldi működésének, szimpatizáns politikai csoportosulások, pártok finanszírozására.

A hálózatban korrupciós célra mozgatott pénzeszközöket egyébként meglehetősen visszás humorérzékkel „alkotmányos költségként”³⁶ tartotta számon a magyar szolgálat. A Metalimpex gyakorlati működése kapcsán pedig egy, a mai szemmel offshore-nak nevezhető cégháló egyes elemei tárulnak. Talán meglepő módon a korabeli szaksajtónak is „feltűnhetett,” hogy 1970-től valami történt a Metalimpex gazdálkodása körül.

A Világgazdaság 1971 augusztusi számában már az olvasható, hogy „1971 első felében a METALIMPEX tőkés forgalmának mérlegében az aktívum a korábbi évekhez képest jelentősen csökkent és kedvezőtlenül befolyásolta a népgazdaság fizetési mérlegét. A tőkés export értéke 23,6 százalékkal kevesebb, mit a múlt év hasonló időszakában volt.”³⁷

Gergely Miklós a tőkés exportbevételek megcsappanását USA-recesszióval, pszichológiai tényezőkkel, globális piaci áreséssel indokolta. Érdekes elemezni a korabeli cikk megfogalmazását is. A Metalimpex váratlan exportbevétel-kiesése ezek szerint olyan mértékű volt, hogy közvetlenül és negatívan befolyásolta az egész magyar népgazdaság fizetési mérlegét.

A fentiek tükrében talán nem alaptalan a feltételezés, hogy a Metalimpex 60-as évek második felétől kezdődő gyökeres átalakítása, a külföldi utazásokkal történő „helyzetbe hozása”,³⁸ majd a 68-69-es exportsikerek (amelyek mögött egyelőre nem ismert megállapodások és mechanizmusok is szerepet játszhattak) egész egyszerűen túl fontos tényezőjévé tették a vállalatot a magyar gazdaság életében, aminek a „megcsapolása” így már túl sok érdeket sérthetett.

³⁵ ÁBTL 3.1.9. V-160338/7., 1974. június 27., 49. old.

³⁶ Például: BORVENDÉG Zsuzsanna: Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016., 115. old. <http://real-phd.mtak.hu/456/1/Borvend%C3%A9gZsuzsanna.pdf> (Megtekintés: 2017.08.15)

³⁷ Világgazdaság, 1971 augusztus 28., Miért csökkent a kohászati termékek exportja?, 3. old.

³⁸ A Magyar Népköztársaság belügyminiszterének 009. számú utasítása a Győr megyei Rendőr-főkapitányság tekintetében például speciális együttműködést írt elő az MNVK-2-vel.

Mindazonáltal elképzelhető az is, főleg az MNVK-2 sajtón belüli aktív jelenléte miatt, hogy igazából nem is „számonkérés” történt, pusztán egy „fedősztori” csillapította az egyébként is mérsékelt kritikák megjelenésének esélyét. Az is bizonyos, hogy az MNVK-2 szorosan együttműködött a KGB-vel, illetve még inkább a GRU³⁹-val, talán a legjobban az összes hasonló szerv közül.

Az Olaszországban különösen aktív Metalimpex, a KGB/GRU és az MNVK-2 szorosabb együttműködése következhetett a Varsói Szerződés (VSZ) tagállamainak „feladatmegosztásából” is, miszerint a Magyar Néphadsereg volt a felelős⁴⁰ az olaszországi NATO bázisok megfigyeléséért.⁴¹

A BM korabeli megállapítása szerint a jutalékrendszeren alapuló üzletfél kiválasztások az évek során – csak a Metalimpex esetében – több millió dolláros veszteséget okoztak a Magyar Népköztársaság számára.⁴² A BM pedig gyakorlatilag már 1973 nyár végére elég információval rendelkezett ahhoz, hogy tisztában legyen Dévai István és Gergely Miklós törvénytelenes tevékenységével.

Érdekesség, és a feltételezett politikai érintettséget talán jól jelzi, hogy 1973-ban Losonczy Pál (a Magyar Népköztársaság Elnöki Tanácsának akkori elnöke) még ki is tüntette Gergely Miklóst a Munka Éremrend arany fokozatával, noha akkor a legfelsőbb körök már pontosan tudhatták, hogy a BM látókörébe került az illegális tevékenységei miatt.

Az MNVK-2 bábáskodása (a BM eljárását folyamatosan „zavarta” a katonai elhárítás érintettsége) ellenére – és annak ellenére, hogy Gergely Miklós egyenesen Biszku Bélától kért⁴³ személyes meghallgatást – végül egyikőjük sem került el a büntetőjogi felelősségre vonást, és a bíróság 1975-ben csempészet, vámor-gazdaság és vesztegetés elkövetése miatt elítélte őket. Dévai Istvánt emellett devizagazdálkodást súlyosan sértő bűntettben is bűnösnek találták.

Dr. Borvendég Zsuzsanna szerint a Dévai-ügy esetében több személyről is szó lehetett, akiknek érintettségét annyira takarni kellett, hogy nevük konkrétan elő sem fordul a dokumentumokban, csak néhány elszórt fordulat utal arra, hogy miniszterek és a párt felső vezetéséhez tartozó személyek is kedvezményezettjei voltak az ismertetett bonyolult korrupciós mechanizmusnak.

³⁹ Felderítő Főcsoportfőnökség (GRU – Главное разведывательное управление), Oroszország (korábban a Szovjetunió) katonai hírszerző szolgálata

⁴⁰ A magyar-olasz kapcsolatokról, konfliktusokról részletesebben Andreides Gábor: *A magyar-olasz kapcsolatok története 1956-1989.*, Budapest, 2008., 68. old. <http://doktori.btk.elte.hu/hist/andreides/diss.pdf> (Megtekintés: 2017.09.30)

⁴¹ BORVENDÉG Zsuzsanna: *Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016., 117. old.* <http://real-phd.mtak.hu/456/1/Borvend%C3%A9gZsuzsanna.pdf> (Megtekintés: 2017.08.15)

⁴² *uo.* 120. old.

⁴³ *uo.* 151. old.

A fent bemutatott, konkrét ügy kapcsán a rivalizálásra utaló konkrét kijelentéseket is lehet a levéltári anyagok között találni. Az MNVK-2 külföldi ügyködését BM-es kiküldöttek általában nem igazán tudták korlátozni és ez talán frusztrációt okozhatott a szervezetben. „Mindenki sérthetetlen volt, aki a katonák körében ténykedett és tett valamit.”⁴⁴

Másik oldalról az MNVK-2 részéről úgy érezhették, hogy „(...) a belügynek egyetlen szerepe van, hogy csak azt kutassa, ki miben ténykedik a kirendeltségen, ki mit csinál olyat, amibe esetleg a belügy beleköthet.”⁴⁵, vagy ahogy más-kor fogalmaztak: „a BM-nek ütkártyára van szüksége a HM elleni hatalmi harcban.”⁴⁶

Mindezek ellenére – talán a kevés forrásra tekintettel – az nem állítható, hogy a rendszerváltozás előtti teljes időszakot végig a rivalizálás jellemezte volna, mint ahogy az sem, hogy az általános jellegű volt. Azonban egyedi konfliktusok, mint az a fentiekből egyértelműen következik, egészen biztosan kialakultak.

Utóélet

A Metalimpex, amely tehát monopóliuma révén fénykorában a teljes magyar acélipar, továbbá színesfém-, alumínium- és golyóscsapágy-kereskedelem export-importját végezte, 1991. december 31-ig működött. Megmaradt vagyonát egy korlátozott felelősségű társaságba, a Metal Vagyonkezelő Kft-be apportálták, a jogutód felszámolása csak 1994-ben indult, és végül csak 2000-ben fejeződött be.⁴⁷

A Metalimpex „hagyatékában” több nagy értékű ingatlan is szerepelt, ezek között is kiemelkedő értéket képviselt egy 3.243 négyzetméter hasznos alapterületű, Budapest V. kerületi irodaház. Ezt az épületet még a felszámolási eljárás előtt értékesítették egy, a részleteiben is megismerhető szerződés⁴⁸ alapján.

A vevő a Budapesti Közép-Európai Egyetem Alapítvány volt, az adásvétel pedig 1992. július 31-én zajlott le. A szerződés aláírását követően 160.000.000 forintot fizetett az alapítvány. A vételárból fennmaradó 180.000.000 forint vételár-rész fejében pedig az alapítvány az eladóra engedményezte „az eladó tájékoztatása szerint a Kormány által jóváhagyott” követelését. Az engedményezett követelés eredeti jogosultja a Soros Alapítvány volt.

⁴⁴ ÁBTL 3.1.5. O-16586/2., 1974. szeptember 26. 210. old.

⁴⁵ uo.

⁴⁶ ÁBTL 3.1.5. O-16586/2., 1974. augusztus 29. 137. old.

⁴⁷ <http://www.napi.hu/redirectedbyprint/titleunknown.19029.html> (Megtekintés: 2017.08.15)

⁴⁸ http://www.kka.hu/soros/Soros_evkonyvek.nsf/11fcbf9d3d07fd42c1256d3600346085/01cc0406dd6dc6e2c1256d6d003f576d?OpenDocument (Megtekintés: 2017.08.15)

Az épület adásvételét jelentő ügylet nem sokkal később az Állami Számvevőszék (ÁSZ) vizsgálata alá került egy, a Művelődési és Közoktatási Minisztérium fejezet pénzügyi-gazdasági ellenőrzéséről szóló 1992. decemberi ÁSZ jelentés alapján.⁴⁹ A tranzakcióval kapcsolatban az Állami Számvevőszék annyit írt, hogy „megjegyezzük, hogy a vételárként kifizetett 160 millió Ft és az alapítvánnyal szemben fennállt 164 millió Ft jogos költségvetési tartozás együttes összege megközelíti az épület korábban más viszonylatú értékesítéséhez megállapított korrigált vagyonértékét.”⁵⁰

A teljes Metalimpex-végelszámolásból – a sajtó szerint⁵¹ – végül 600 millió forinthez jutott az ÁPV Rt. A politikai rendszerváltozás során a korábbi állambiztonsági rendszert⁵² új nemzetbiztonsági struktúra váltotta fel:⁵³ 1990-ben megalkult a Honvéd Vezérkar Katonai Felderítő Hivatal és a Magyar Honvédség Katonai Biztonsági Hivatal.

⁴⁹ Állami Számvevőszék: *Jelentés a Művelődési és Közoktatási Minisztérium fejezet pénzügyi-gazdasági ellenőrzéséről*, 1992. december, <https://www.asz.hu/storage/files/files/%C3%96sszes%20jelent%C3%A9s/1996/131j000.pdf> (Megtekintés: 2017.08.15)

⁵⁰ *uo.* 31. old.

⁵¹ <http://www.napi.hu/redirectedbyprint/titleunknown.19029.html> (Megtekintés: 2017.08.15)

⁵² <http://www.defence.hu/container/files/9/4954/abrak.pdf> (Megtekintés: 2017.08.15)

⁵³ <http://www.knbsz.qov.hu/hu/tortenete.html> (Megtekintés: 2017.08.15)

Irodalomjegyzék:

- ANDREIDES Gábor: A magyar-olasz kapcsolatok története 1956-1989., Budapest, 2008.
- BORVENDÉG Zsuzsanna: Újságírók és külkereskedők a Kádár-rendszer hírszerzésében, Állambiztonsági Szolgálatok Történeti Levéltára Kutatási Osztály, Budapest, 2016.
- Dr. HAJMA Lajos: A katonai felderítés és hírszerzés története, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2001.
- MAGYAR Balázs: A magyar katonai hírszerzés tevékenységének fő irányai és jellemzői a versói szerződés időszakában, Budapest, Hadtudományi Szemle 2008/2.
- NAGY Gyula: A magyar katonai képzések története (1945 – 1990), Budapest, Nemzetbiztonsági Szemle, 2014. Különszám I.
- ÁBTL 3.1.5. O-16586/2., 1974. szeptember 26.
- ÁBTL 3.1.5. O-16586/2., 1974. augusztus 29.
- ÁBTL 3.1.9. V-160338/7., 1974. június 27.

A hír, az adat, az információ és a dokumentáció fogalma, helye, szerepe a döntéshozatalban

Dr. Jávor Endre¹

Absztrakt:

Korszerű viszonyok között a nemzetbiztonsági tevékenység feladata, rendeltetése a felső szintű politikai, biztonságpolitikai, katonai döntéshozatalhoz szükséges ismeret, tudás elemeinek, összetevőinek megszerzése, ezek feldolgozása és a feladattámasztó, döntéshozó szervek részére történő rendelkezésre bocsátása. Az ismeret, tudás, információ megszerzése hatékonyságának, eredményességének egyik fontos feltétele, kritériuma a tudományos igényesség. Ezen a ponton kell feltenni azt a kérdést, hogy azok a szakkifejezések, melyeket a nemzetbiztonsági tevékenység elemeként axiomatikusan használunk, ismerünk, mennyire felelnek meg annak a tevékenységnek, amit megjelenítenek, képviselnek. A döntéshozatal támogatásának eszköze nem a titkos módszerekkel megszerzett hír, hanem az ismert, tudást tartalmazó, információvá feldolgozott, az információigény tartalmi kritériumai által determinált módszerekkel megszerzett hírek, adatok összessége, ahol az információ valóságtartalma, felhasználhatósága, minősége az elemző, értékelő, munka minőségének függvénye.

Kulcsszavak: tudatosság, ismeret, tudás, információ

Abstract:

Under modern conditions, the task of the national security activity is to acquire the knowledge, the elements and components of the knowledge required for the top level political, security policy and military decision-making, the processing of them and the provision of the task support, decision-making bodies. An important condition for the efficiency and effectiveness of obtaining cognition, knowledge and information is the criterion of scientific excellence. At this point, the question is whether the terms used and known as axiomatically in the element of national security activity how well they correspond to the activity they represent and incarnate. The means of supporting decision-making are not the news obtained by secret methods, but the content of the information that has been disclosed and processed for information, obtained through methods determined by the content criteria of the information request, where the reality, the usability and quality of information is a function of the quality of analysis, evaluation.

Keywords: awareness, cognition, knowledge, information

¹ ORCID azonosító: orcid.org/0000-0001-6200-9025

Bevezető gondolatok

Korszerű viszonyok között a nemzetbiztonsági tevékenység feladata, rendeltetése a felső szintű politikai, biztonságpolitikai, katonai döntéshozatalhoz szükséges ismeret, tudás elemeinek, összetevőinek megszerzése, ezek feldolgozása és a feladattámasztó, döntéshozó szervek részére történő rendelkezésre bocsátása. Ebben az összefüggésben merül fel a kérdés, hogy azok a szakkifejezések, melyeket a nemzetbiztonsági tevékenység axiomatikusan használt elemeiként ismerünk, mennyire felelnek meg annak a tevékenységnek, amit megjelenítenek, képviselnek. Másképpen fogalmazva, hogyan, milyen kifejezésekre épül fel a döntéshozatalba beépítésre kerülő tudás és ismeret.

Számomra fontos emberektől azt tanultam, hogy az ember első számú joga a kételkedés, a visszakérdezés akár olyan axiomatikusan használt "igazságokra" is, melyek első megközelítésben magától értetődőnek tűnnek. Ugyanakkor úgy vélem az ember első számú kötelessége a kételkedéseire a válaszok, a megoldások konzekvens keresése.

Ebben az írásban arra keresek választ illetve megoldást, hogy amikor a „hírszerzés” kifejezést használjuk, akkor az valójában mennyire fedi le, milyen viszonyban van az általa megtestesített, megjelenített folyamattal, tevékenységgel. Mielőtt azonban a szó, a kifejezés közvetlen morfológiai, lexikológia értelmezését vizsgálánánk, először azt a funkciót, tevékenységet kell vizsgálni, amelyet a társadalomban betölt, amelyet a társadalom hol axiomatikusan, hol vitatkozva elfogad, és megért. Ennek során foglalkozom a tudatos tevékenység kialakulásával, illetve a döntéshozatalt támogató információ részelemeinek tartalmi és formai fejlődésének folyamatával.

Ez az írás azoknak szól, akik a misztifikáción, a konspirációs szemléleten túlmenően is kíváncsiak a nemzetbiztonsági tevékenységre, akik természetes valóságában szeretnének betekintést nyerni a döntéshozatalt támogató információszolgáltatás rendszerébe. Ez az írás egy kísérlet annak bemutatására, hogy az információ, a tudás, az ismeret, mindaddig, ameddig nem célja, hanem eszköze a döntéshozatalnak, nem más, mint egy természetes emberi algoritmus. Ennek ugyan vannak különleges esetei, regényekben, filmekben illő kalandos történetei, de izgalmas eseményekkel, konfliktusokkal és a „jó” győzelmével végződő történetekkel a tudományos felfedezésektől a bünygyi regényekig az élet minden más területén is találkozunk. Ha a nemzetbiztonsági tevékenység társadalmi elfogadottságát fontosnak és szükségesnek tarjuk, akkor be kell mutatni, érzékeltetni kell, hogy ez a tevékenység demokratikus társadalmi viszonyok között tendenciájában nem hatalmi, hanem szolgáltató funkciót tölt be. Ha ki akarjuk elégíteni azt a jogos igényt, hogy a társadalom ismereteket szerezzen a nemzetbiztonsági

szolgálatok, tevékenységéről, akkor be kell mutatni azokat az összefüggéseket, melyek a politikában, biztonságpolitikában és a tudományos-technikai szférában végbement változások világában érthetővé, és értelmezhetővé teszik az elmúlt évtizedekben szükségessé vált, illetve bekövetkezett szemléleti változásokat.

A tudatos tevékenység kialakulásának folyamata

Minden emberi tevékenység alapja a biológiai lét során kialakult és társadalmi szinten továbbfejlődött szükségletek, valamint a társadalmi lét következtében kifejlődött és folyamatosan továbbfejlődő tudatosság.

Az emberi tevékenység célja és az egymásközi kapcsolattartás, kommunikáció alapvető tartalma a biológiai eredetű szükségletek kielégítése. A „biológiai” ebben az összefüggésben azt jelenti, hogy a túlélés, a lét fenntartása ezeknek a szükségletek kielégítésének függvénye. Maga a biológiai szükséglet kielégítése – pl. táplálkozás, pihenés, nemzés, egy az életet, vagy testi épséget veszélyeztető támadás elhárítása – egyedi, egymástól térben vagy időben elkülönülő aktusok sorozata, de a feltételek megteremtése egy állandóan ismétlődő, megújuló folyamat. Mint ilyen tele van bizonytalansággal, melyek akár a feltételek részleges vagy teljes megsemmisülését, esetleg hibás vagy hiányos teljesülését eredményezhetik. A feltételek a társadalmi, technikai-tudományos fejlődés eredményeképpen egyre bővülnek, egyre összetettebbé válnak, és kölcsönhatásba lépnek egymással. Ennél fogva kielégítésük is egyre fontosabbá, ugyanakkor egyre összetettebbé és bonyolultabbá válik. A létfenntartás, a túlélés akkor kerül veszélybe, ha a feltételek kielégítése akadályokba ütközik, végső esetben lehetetlenné válik. A társadalom, a tudomány és technika fejlődésével párhuzamosan a veszélyek is egyre összetettebbé, egyre áttételesebbé válnak.

A veszélyt, a fenyegetettséget első fokon és közvetlen formában az ember örökölt biológiai ösztönei – látás, hallás, szaglás, érzékelés – segítségével ismeri fel. A veszély felismerése egyrészt az előzetes tapasztalatokon, másrészt azon alapszik, hogy valami, korábban ismeretlen – feltehetőleg – fenyegetést tartalmazó jelenség történik. Ilyen esetben az első reakció a félelem, mely egyrészt lebéníthat, pánikot okozhat, de ugyanakkor a józan óvatosság forrása lehet. E két hatás együttes következményeként az ember ugyancsak örökölt biológiai ösztönei – gyorsaság, erő, látás, hallás, szaglás, tapintás, rejtőzés, álcázás – felhasználásával védekezik, megelőzi a veszélyt, illetve ellentámadásba megy át. Ez utóbbi reakció nem egyéb, mint az életösztön megnyilvánulása. Az életösztön képezi az alapját annak a tudatosodási folyamatnak, mely a társadalom és a technikai-tudományos fejlődéssel összhangban az emberi élet védelmét egy napjainkban is tartó folyamat részeként egyre magasabb szintre emeli.

Az állatvilágban az egyes fajok a táplálkozási sorrendnek megfelelően felkutatják, megtámadják, üldözik, elfogják és elpusztítják a táplálékot megtestesítő fajhoz tartozó egyedet, illetve védekeznek, menekülnek és ellenállnak az őket

táplálékként elpusztítani szándékozó támadóval szemben. Az ember, mint biológiai lény örökölte, és mint társadalmi lény társadalmasította, tudatos tevékenységgé fejlesztette ezeket az ösztönöket. Az ember akkor jelenik meg, a biológiai lét akkor ér el egy minőségileg magasabb színvonalat, amikor az életösztön által vezérelt cselekvésformák társadalmi keretek között fejlődnek tovább. Az így kifejlődött társadalmi lény, az ember, egyrészt tudatossá, szervezetté fejlesztette a táplálék megszerzésnek módjait, másrészt ellentétben az állatvilággal, már nem csak testi, fizikai adottságait, - gyorsaság, erő, álcázó képesség, éles látás, szaglás, stb. - örökölt ösztöneit alkalmazta a védelemre, menekülésre, illetve támadásra, harcra, hanem – a természeti feltételek és korlátok kompenzálása, illetve erőfölény kialakítása céljából - eszközöket, szerszámokat, fegyvereket fejlesztett ki és használt.

Az alapvető eszközök és szerszámok – tűz, nyíl, pattintott szerszámok, kerék - feltalálása, megalkotása, használata már az összegyűjtött tapasztalatokra épült, feltételezte a tudatosságot, a kreatív gondolkodást, de mindenekelőtt a szükségletek – tudatos - megfogalmazását. Az eszközök kifejlesztése, használata és az ahhoz kapcsolódó tevékenységek, manipulációk köre a társadalmi, tudományos, műszaki-technikai fejlődéssel párhuzamosan folyamatosan fejlődött, kibővült, és elérte azt a fokot, hogy korszerű körülmények között egyik elsődleges probléma már nem a szükségletek kielégítése, hanem a kielégítendő szükségletek fontossági sorrendjének meghatározása.

Az ember a környezetét és az őt érő jelenségeket érzékszervei segítségével a különböző észlelt jelenségek, jellemzők, illetve az azokból levont következtetések és tapasztalatok alapján érzékeli és értelmezi. Ezt követően agyának elemző, alkotó, elvonatkoztató és integráló képességével, valamint a memória aktív segítségével tudatilag modellezi a világ egyes jellemzőit, majd a fantázia, a képzelet segítségével az egyes elemeit, összetevőit ártrendezi, gondolati műveleteket végez velük és új következtetésekre jut.

Az emberek tudomására jutott ismeretek többsége nem közvetlen tapasztalatok útján keletkezik, hanem különböző áttételeken keresztül. Mindaddig, ameddig az emberek a primitív viszonyok között saját magukra voltak utalva, mindent, ami az élet fennmaradásához szükséges volt, saját maguk állítottak elő, végeztek el, és az ehhez szükséges nyersanyagok, táplálék elérhető távolságon belül megtalálható volt, az emberek ismereteinek többsége a közvetlen, átélt tapasztalatok alapján jött létre. Minőségi változást a munkamegosztás, és ezzel párhuzamosan a beszéd kialakulása hozott. Az ember egyik fontos képessége, az emberi tevékenység egyik fontos eleme az egyes események cselekvések, tárgyak, jelenségek, folyamatok, műveletek tartalmának, jellegzetes tulajdonságainak nyelvi formában történő értelmezése, megfogalmazása, megvitatása, továbbfejlesztése. Ez odáig terjed, hogy a társadalmi tevékenység, az emberi élet minősége, hatékonysága messzemenően függ belső összefüggéseinek, jellemző tulajdonságainak, kapcsolati rendszerének adekvát értelmezésétől. Ebben a fo-

lyamatban egyre növekedett az áttételesen megszerzett ismertelemek aránya. A fejlődés tendenciája azt mutatja, hogy napjainkban az egyes ember, vagy a döntéshozók rendelkezésére álló hírek, adatok áttételesen megszerzett, sőt többszörös áttételen keresztül megszerzett ismertelemekre épülnek.

A társadalom fokozatos fejlődésével párhuzamosan kialakulnak az egyes ember mindennapi életére, valamint a közösség tevékenységére jellemző magatartás-, tevékenység- és viselkedésformák. Ezek már magukon hordozzák az emberi tevékenységre jellemző egyrészt racionális, másrészt emocionális cselekvés, tehát az ember belső ellentmondásokkal teli magatartásának elemeit. Az emberi magatartás, az emberi döntéshozatal kiszámíthatatlansága, sok esetben ellentmondásossága a racionális és emocionális elemek egymáshoz viszonyított arányának, továbbá annak a függvénye, hogy a racionális elem milyen fokon tud befolyást gyakorolni az emocionális elemre, illetve az emocionális elem milyen fokon befolyásolja a racionális elemet.

Közösségek viszonyrendszere

Az ember ebben a folyamatban kettős szerepet játszik. Egyrészt az azonos szükségletek kielégítésének folyamatában az azonos, vagy hasonló érdekeket és értékeket képviselő, követő emberek egymással együttműködnek, másrészt az eltérő érdekeket és értékeket képviselő és követő emberek csoportja konkurens, rivalizáló, ellenséges pozíciót foglal el. Az egyes emberek, az emberek különböző – együttműködő, vagy rivalizáló – csoportjai közötti kapcsolatok, a társadalmi tevékenységek különböző formái az információ segítségével, az információ közvetítésével valósulnak meg. Az emberek, amikor találkoznak, kapcsolatba kerülnek egymással, ösztönösen, vagy tudatosan érzékelik egymást, kölcsönösen megtudnak egymástól, vagy egymástól korábban nem ismert dolgokat, esetleg a már ismert dolgokra vonatkozó változásokat. Ezeknek az információknak a birtokában tudnak dönteni a kapcsolat további tartalmáról. Másképpen kifejezve minden kapcsolat egyben információ-szerzési és továbbítási alkalom, lehetőség.

A kapcsolat nem csak azt jelenti, hogy az érdekelt felek egy fizikai térben, egymással közvetlen látó, halló, beszélő távolságban érintkeznek egymással, hanem ennek van egy közvetett formája is. Ilyenkor az érdekelt felek nem kerülnek egymással közvetlen kapcsolatba, de az érdekek, értékek alapján történő együttműködés vagy rivalizálás következtében tudnak egymásról, számon tartják egymást. Ebben a vonatkozásban az információ is kettős szerepet tölt be. Az együttműködőkkel kialakított információszerzés és információcsera a közös célok megvalósítását, az együttműködés fenntartását, fejlesztését, védelmét szolgálja. A riválisok, az ellenség vonatkozásában egyrészt meg kell szerezni a másik féllel szembeni viszony kialakításához szükséges információkat, másrészt védeni kell a saját információkat.

Az információ szerepe

Az információ, különösen az elmúlt évtizedek rohamos technikai fejlődése következtében, a magánélettől a legátfogóbb társadalmi, politikai, védelmi, gazdasági, kulturális, szociális, tudományos, oktatási és egyes területeket is beleértve egyre szélesebb területen tölt be befolyásoló szerepet. Ebben az írásban az információnak a döntéshozatalban betöltött szerepére koncentrálok. Az, hogy koncentrálok, egyben azt is érzékelteti, hogy a döntéshozatalt olyan központi rendező elvnek tekintem, mely messzemenően figyelembe veszi az információ többi aspektusainak befolyásoló szerepét is.

Az egyes ember napi életéhez, csakúgy, mint társadalmi szinten a politikához, védelemhez tartozó feladatok – először ösztönös, később egyre tudatosabbá váló – ellátáshoz folyamatos döntésekre, döntéshozatalra van szükség. A döntéshozatal kiinduló eleme a szükségletek, illetve az azokból levezetett érdekek és értékek megfogalmazása. Az érdekek és értékek² képezik a célkitűzések, illetve azok eléréséhez szükséges feladatok meghatározásának alapját. Ebben a folyamatban történik annak meghatározása is, hogy az adott feladatok végrehajtásához, a célkitűzések eléréséhez, végső fokon a döntéshozatalhoz milyen információkra van szükség.

A korai időkben az információk mindenekelőtt az alapvető életfeltételek, a biológiai szükségletek kielégítését, az élelemszerzés, a természeti jelenségekkel szembeni védekezés céljait szolgálták. Később, ahogy a munkamegosztás és az eszközök, szerszámok, fegyverek, védőeszközök, a társadalmi tevékenység rendszere fejlődött, úgy fejlődött a döntéshozatal során felhasználható információ tartalma, megjelenési formája, és természetesen az információk feldolgozásának módszertana is. Minél szélesebb körűvé fejlődik az emberi tevékenység, egyrészt annál több igény, szükséglet jelenik meg, másrészt annál több döntésre van szükség. Következésképpen jelentősen megnő az információigény. A döntéshozatalhoz szükséges információk megszerzése, elemzése, értékelése, felhasználása, valójában egy természetes emberi cselekvési algoritmus, éppúgy, mint bármely más biológiai eredetű, de társadalmivá vált emberi tevékenység, pl. az utódok nevelése, az élelem megszerzése, és mint ilyen, elengedhetetlen az adott társadalmi tevékenységi terület tartalmi, szakmai, tudományos igényességgel feldolgozott információinak alkalmazása, felhasználása a döntéshozatal során. Az információk a politikai szintű döntések racionális, tartalmi, szakmai alapját testésítik meg. Az információ minden döntéshozatal alapvető, integráns eleme, ezért az információ igényt és szükségletet a döntéshozatal szintjén kell meghatározni.

² Nem mindegy a sorrend.

A történelem feltehetőleg első, és rendelkezésünkre álló információigény meghatározásáról a Bibliában az alábbiakat olvashatjuk:

„1. És szólt az Örökkévaló Mózeshez, mondván: 2. Küldj el férfiakat, hogy ki-kémleljék Kanaán országát, amelyet én Izráel fiainak adok; egy-egy férfiút küldjete-
tek atyáik törzséből, mindazt, aki fejedelem közöttük. 3. És elküldte őket Mózes
Párán sivatagából az Örökkévaló parancsára; mindnyájan olyan férfiak, akik Izrá-
el fiainak fejei. ... 17.

És elküldte őket Mózes, hogy kémleljék ki Kanaán országát; és mondta nekik:
Menjetek föl erre a déli vidéken és menjetek föl a hegyek közé, 18.

és nézzétek meg az országot, milyen az és milyen a rajta lakó nép, vajjon
erős-e vagy gyenge, kevés-e vagy sok; 19.

és milyen az ország, amelyben laknak, vajjon jó-e vagy rossz; és milyenek a
városok, amelyekben laknak, vajjon táborokban vagy várakban; 20.

és milyen a föld, vajon kövér-e vagy sovány; van-e benne fa vagy nincs? Le-
gyetek bátrak és hozzatok az ország gyümölcséből.”³

Ebből az idézetből kiolvasható a legfelsőbb szintű politikai igényből, szükség-
letből levezetett feladat-meghatározást, - 1. és 2. pont – a feladatok lebontását,
a végrehajtók kiválasztását, - 3. pont – valamint a végrehajtás szintjére lebontott
hír- és adatszerzési feladatok meghatározását, beleértve a dokumentáció-szerzés
fontosságát is – 17.-20. pont.

Minél inkább eltávolodunk az ösztönös cselekvés szintjétől, minél inkább
összetettebbé válnak a döntéshozatal befolyásoló tényezők, annál inkább elő-
térbe kerül és megerősödik a tudatos, tehát az információn alapuló döntéshoza-
tal fontossága, jelentősége. A tudatos tevékenység alapja a tudás, az ismeret. Az
ismeret alapja a tapasztalat, valamint a valóságra, vagy annak valamely részére,
témájára vonatkozó értesülés, - hír, adat - strukturált feldolgozása útján szerzett,
létrejött információ. Az első tapasztalatok és a jövő tervezésének egyfajta elsőd-
leges változata a periodikusan visszatérő események, jelenségek összefüggései-
nek, következményeinek felismerése volt.

A hír

A „hír” mint szó, mint fogalom nagyon sokféleképpen értelmezhető, nagyon sok
különböző, egymástól eltérő – alapvetően a különböző szakterületekhez kötődő
- megfogalmazása van. Ebben az írásban azt az értelmezést használom, mely
szerint a hír nem egyéb, mint új ismertető közlemény. A hír egy olyan „újdons-
ság”, mely forrásnál, tartalmánál fogva figyelemfelkeltő, és bizonyos körök, tár-

³ Szentírás. Mózes öt könyve. Szerk. Dr. Hertz J.H. Második kiadás. Akadémiai Kiadó Bu-
dapest 1984. IV. könyv, XIII. fejezet 129-131. old. Az idézet szó szerinti, ezért helyenként
nem felel meg a ma érvényes helyesírási szabályoknak.

sadalmi csoportok, szakterületek, célcsoportok érdeklődésére tarthat számot. A hír utalás valamilyen esemény valószínűségére. Ha elemezzük az információszerzés történelmét, tapasztalatait, arra a következtetésre jutunk, hogy a legértékesebb, legfontosabb védett, minősített információk háttérében a kiindulás, a feladattámasztás és megfogalmazás szintjén megtaláljuk a hírt, mégpedig a nyílt, mindenki⁴ számára elérhető forrásból származó, bárki számára alkalmazható – kockázatmentes, törvényes - módszerek segítségével megszerzett hírt. Az információs kultúra és technológia fejlődésének egyik sajátossága, hogy soha nem látott mértékben és tömegben megnövelte a nyílt források számát és elérhetőségét. Történelmi tény és fontos tapasztalat ugyanakkor, hogy a klasszikus hírszerzésben a nem titkosszolgálati módszerekkel szerzett híreknek, adatoknak a korábbi időszakban nem volt értéke. A korszerű hírszerzés, információszerzés egyik fontos kritériuma a nyílt forrású hírek értékének felismerése, illetve a módszer-centrikus szemléletről a tartalom-centrikus szemléletre történő áttérés.

A hír funkciója az aktuális eseményekre történő figyelem felkeltése, továbbá veszélyjelzés, illetve háttér-ismeret biztosítása. Abból az elméleti feltételezésből kiindulva, hogy meghatározott területekről nulla információval rendelkezünk, foglalkozni kell a hírral, mint nyers, elsődleges, figyelemfelkeltő ismeretelemmel. A hír rövidege mellett az egyik frontos sajátossága az azonnali megérthetőség. A hír tehát egy új, friss, figyelemfelkeltő eseményre vonatkozó közlemény, egy elsődleges értelmét gyorsan felfogható ötlet, gondolat realizálása, megfogalmazása, mely alkalmas arra, hogy a hírral kapcsolatos további, most már strukturált, vagy esetleg strukturálatlan formában megjelenő adatok megszerzésére ösztönözzön.

A hír megjelenési formája lehet hallomás, szóbeli közlemény,⁵ „brainstorming”, más hír, adat, információ mellékterméke, töredéke, része.⁶ A hírek forrásai az interneten, újság-, és televíziós híreken túlmenően – a teljesség igénye nélkül - felölelik a piackutatásokat, közvélemény-kutatásokat, tudományos publikációkat, folyóiratokat, találmányokat, kutatások eredményeit, folyamatban levő kutatások részeredményeit, a versenyszféra és gazdasági folyamatok eredmény-kimutatásait, beszámolóit, elemzéseit, propaganda anyagokat, irodalmi és művészeti alkotásokat.

Vannak olyan hírek, melyek csak az emberek fejében jelennek meg, realizálódnak, öltenek formát, állnak össze, mert a hozzájuk tartozó motiváció, érzelem, másodlagos értelmezés nem komputerizálható. Napjainkban a nagytömegű és egymással közvetlenül, vagy áttételesen összekapcsolódó adatok, információk világában jószerével nem találni olyan eseményt, tényt, jelenséget, melynek ne lenne valahol, valamilyen formában előzménye és teljes újdonságként jelenne

⁴ Mindenki, aki az adott témával foglalkozik, vagy az iránt érdeklődik.

⁵ Pl. fogadáson történő beszélgetés, spontán beszélgetés.

⁶ Pl. tudományos konferencián hallott előadás más összefüggésbe helyezése.

meg.⁷ Ennek ellenére nem lehet figyelmen kívül hagyni azt az elméleti lehetőséget, hogy különösen az emberi közlések szférájában olyan új szempontok, tevékenységi területek jelennek meg, melyek figyelemfelkeltőek, és bizonyos értelemben, bizonyos összefüggésben az újdonság erejével hatnak.⁸ Az ma már természetes, hogy egy címszó hallatán azonnal meg lehet kezdeni a keresést az interneten, de a címszóig is el kell valahogy jutni. Ez tulajdonképpen a „hír” eredeti rendeltetése.

A történelmi tapasztalatok azt mutatják, hogy a nyers hírek a döntéshozatal folyamatában ellentmondásos szerepet játszottak. A korai társadalmak idejében, amikor a hírek továbbítása, illetve a továbbított hírek terjedelme a fejletlen kommunikációs feltételek miatt korlátozott volt, maga a nyers hír volt a döntéshozatal szinte egyetlen információt tartalmazó háttere. Amennyiben a hír tartalma megfelelt a döntéshozó - uralkodó - elvárásainak, előítéleteinek, akkor függetlenül annak valóságtartalmától azt beépítette a döntésbe. Ellenkező esetben, ugyancsak függetlenül a valóságtartalomtól, amennyiben a hír nem nyerte meg a döntéshozó tetszését, döntése során azt figyelmen kívül hagyta.⁹

Ugyanarra az eseményre vonatkozó hír több, egymástól független forrásból is származhat, ami erősen valószínűsítheti, vagy vitatja a hír valóságtartalmát, és ösztönözheti a hírre vonatkozó adatok megszerzésének szükségességét. A hír fontos eleme, hogy megjelöli az adatok elérhetőségének irányát, forrását, bizonyos értelemben a források elérhetőségét.

Napjainkban a világ bármely táján történő, biztonságpolitikai vonatkozású események a globális hálózattal rendelkező hírcsatornák, hírügynökségek - pl. CNN International, FOX News, internetes hálózatok, stb. - útján szinte az eseményekkel egy időben elérhetők, amit a hivatalos információszerző szolgálatok is messzemenően kihasználnak. Ez a lehetőség azonban az információszerző folyamatnak csak az első lépése. Gyorsaságban ezekkel a hírcsatornákkal versenyezni nem lehet, de az általuk szolgáltatott hírek, éppen a gyorsaságból eredően csak kiinduló forrásai lehetnek az adatgyűjtésnek, adatszerzésnek.

Az adat

⁷ Éppen ezért hasznos, szükséges és lehetséges egy, az információk megszerzésére vonatkozó hipotézis felállítását.

⁸ A sakktáblán 64 mező és 32 bábú található, a sakkot több ezer éve játssza az emberiség, a magas szinten sakkozók fejében játszmák százai rögződtek, mégis előfordul, hogy egyik játékos meg tudja lepni a másikat.

⁹ Érdekes tanulság a szovjet-német háború kitörésének előzménye. Sztálin több forrásból – Sorge, Radó Sándor, Churchill – megkapta az adatokkal – időpont, támadási irányok, felvonultatott erők, politikai célkitűzések – is megerősített hírt, de mivel a hírt nem fogadta el, nem érdekelték a hírt alátámasztó adatok.

A hír, legyen az bármilyen figyelemfelkeltő, első hallásra rendkívül fontosnak tűnő, önmagában nem képvisel értéket a döntéshozatalt támogató információ-szerzés szempontjából. Nem a hír hordoz értéket, hanem a hozzá tartozó, a hírt információ elemévé fejlesztő adatok, illetve az adatok rendszere. A hír akkor válik értékké, akkor állapítható meg elsődleges értéke, ha megjelennek a hírre vonatkozó adatok. Mindaddig, ameddig a hír értékét adatok nem erősítik meg, addig a hír nem több mint hallomás, pletyka, szóbeszéd, legfeljebb figyelemfelkeltés. Ugyanarra az eseményre vonatkozó hír az eltérő források érzékelése függvényében lehetnek ellentmondásosak, felületesek. (Pl. szemtanúk vallomásai, megfigyelései egy közlekedési baleset esetén.)

A hír akkor válik értékessé a döntéshozatal szempontjából, ha a hozzá tartozó adatok alapján értelmezhető valós értéke, szerepe, hasznossága. A megszerzendő információk gazdái, tulajdonosai, létrehozói nem elsősorban a hírre, mint tényre, eseményre érzékenyek, nem annak eltitkolását tartják fontosnak, hanem az adott hírre vonatkozó adatokat. Ezért vagy a minimális, feltétlenül szükséges mennyiségű adatot tesznek elérhetővé, vagy megtévesztő adatokat publikálnak. Ez az eljárás mindaddig eredményes lehet, ameddig egy rendszer nem kezd el működni, és működésének eredményei, következményei nem lesznek érzékelhetők. (Pl. Csernobil.)

Egy olyan hír, aminek nincs érzékelhető következménye, elhal, érdektelenné válik. A valódi, értékes hír, abban a pillanatban, amikor megjelenik, máris hiányérzetet kelt, kérdéseket indukál. Egy hír akkor bizonyul reálisnak, valósnak, figyelemre és további feldolgozásra alkalmasnak, ha az általa megjelölt eseményeknek, történeteknek a valós, vagy várható, de mindenképpen befolyásoló hatása, következménye érzékelhetővé, értelmezhetővé válik.¹⁰ A kérdések a hírek, események, történetek alapvető paramétereire – ki, mit, mikor, hol, miért, hogyan – illetve belső összefüggéseire, továbbá kapcsolati és viszonyrendszereire irányulnak. Ezeknek a kérdéseknek a megválaszolása első fokon az adatok gyűjtésének, fejlettebb szinten az adatok megszerzésének a funkciója.

Az adatnak, mint fogalomnak az értelmezése, használata az információs kultúra fejlődésével párhuzamosan rohamos fejlődésnek indult, folyamatosan bővül, és egyre szélesebbé, sokoldalúbbá válik. A Hadtudományi Lexikon megfogalmazása szerint az adat valamely hír, ismeret megértését, alkalmazását elősegítő, alátámasztó, magyarázó mérhető, összehasonlítható, ellenőrizhető paraméterek, jellemzők összessége.¹¹ Másképpen kifejezve az adat a hír hozzáadott értéke, illetve az értékelő, elemző, feldolgozó tevékenység alapeleme.

Az Egyesült Államok katonai értelmező szótára szerint az adat tények, koncepciók, ismeretek meghatározott formában történő megjelenítése, mely alkalmassá teszi ezeket, emberek által vagy automatizált eszközök útján történő to-

¹⁰ Ezzel együtt meg kell felelni az információigény feltételeinek is.

¹¹ *Hadtudományi Lexikon. Magyar Hadtudományi Társaság. Budapest 1995. p. 4.*

vábbításra, értelmezésre, műveletek végzésére. Adat minden olyan jel, jelzés, mennyiség, melyhez valamilyen értelmezés, magyarázat fűzhető.¹²

Az adat kifejlődése

Az adat, mint fogalom akkor válik értelmezhetővé, ha megismerkedünk történelmi fejlődésével. Az írásbeliség kifejlődése előtti időszakban a hír forrása a megfigyelés, illetve a forráslehetőséggel, a helyzetükből, adottságaikból, kapcsolati rendszerükből eredően feltehetőleg fontos ismeretekkel rendelkező személyekkel történő beszélgetés volt. Ilyen körülmények között nem a hírek megszerzése, hanem - a kezdetleges közlekedési, hírközlési feltételek mellett - annak továbbítása, a döntéshozóhoz történő eljuttatása volt a fő megoldandó probléma. Ugyanakkor nagyon fontos volt a hírek pontossága - valóságtartalma - illetve időszerűsége. Az írásbeliség hiánya nem csak azt jelentette, hogy nem voltak betűk és számok, egyezményes jelek, hanem azt is, hogy hiányoztak a feljegyzések, közlemények rögzítéséhez nélkülözhetetlen eszközök, az adathordozók is. Ennek egyik következménye az volt, hogy a megszerzett hírek rövidek, a megjegyezhetőség által korlátozott terjedelműek voltak, és a továbbítás során, ahány állomáson, közvetítőn keresztül mentek, mindannyiszor fennállt a torzulás veszélye. Az időszerűség a kezdetleges, fejletlen közlekedés viszonyok függvénye volt, és fontos hírek gyakran későn érkeztek meg, vagy csak nagyon kevés idő maradt a feldolgozásra, felhasználásra, döntéshozatalra.

Alapvető minőségi változást az írásbeliség megjelenése hozott. Az írásbeliség első eredménye és következménye az emberi agy korlátozott tároló képességének túllépése, és egy külső emlékezeti, tárolási lehetőség létrehozása.¹³ Az első és legfontosabb változás, hogy lehetővé vált a hírszerző és a feladatszabó-felhasználó közötti egyezményes jelek segítségével történő üzenetváltás, más-képpen kifejezve a megszerzett hír rögzíthető, nagy távolságra eljuttatható és hosszú időre megőrizhető. A hírek továbbításának már nem szabott terjedelmi határt az emberi emlékezőképesség, és a tartalmi, pontossági kritériumok szintje jelentősen megnövekedett. De további fontos változás volt az is, hogy a megszerzendő és megszerzett hírek egyrészt túllépték a szóbeliség korlátait, kiterjedtek az írásos anyagok megismerésére, megszerzésére is.

Az adatok megjelenését onnan lehet számítani, amikor írásos anyagok már nem csak a nyers hírt, hanem az azt kibővítő, minősítő, értelmező ismereteket is

¹² JP1-02, *Department of Defense Dictionary of Military and Associated Terms*; 8 November 2010. (Amended Through 15. April 2012.) p. 83.

¹³ KALLA Gábor: Az írásbeliség kezdetei és a korai írásbeliség társadalmi beágyazottsága. (http://qepeskonyv.btk.elte.hu/adatok/Okor-kelet/Okori.es.keleti.nyelvek.es.irasok/index.asp_id=159) (letöltve: 2012.07.20.)

tartalmazták. Az írásbeliség megjelenése egyrészt lehetővé tette a megfigyelések, illetve megszerzett szóbeli ismeretek eredményeinek adatokkal történő kibővítését, másrészt az adatok egyezményes jelek, szimbólumok formájában történő hosszú távú rögzítését, megőrzését, ami egyúttal az adatbázisok kezdetleges megjelenése volt. Ennek egyenes következménye volt az adatszerűség kialakulása, ami azt jelenti, hogy a megszerzhető ismeretek, hírek valódiságát, hitelességét, megértését, dokumentumok támasztják alá. Fontos elem volt a mérhetőség, a mértékegységek, ekvivalens értékek megjelenése, mely lehetővé tette a jelenségek, események, folyamatok jellemzőinek, tulajdonságainak, paramétereinek meghatározását, és ez által a hírekhez kötődő adatok értelmezését. Egy további fontos következmény volt, hogy az adatokkal kibővített hírekkel már műveleteket lehetett végezni, ami megalapozta az elemző, értékelő munkát, illetve a tervezést.

Az adat formái, tartalmi összetevői a társadalmi tevékenységek, illetve a tudományos, műszaki-technikai fejlődés következtében jelentős minőségi változáson mentek keresztül. Az adatszerzést, a kezdeti empirikus feltételeket folyamatosan fejlesztve, napjainkban jelentős mértékben a különböző érzékelő, informatikai rendszerek, illetve azok kombinációi végzik. Az adathordozók kezdetleges formája még nem tette lehetővé az adatok továbbítását, pontosabban kifejezve egyfajta statikus adattárolást tett lehetővé. Közismert, hogy az első ember által készített, az írásbeliség közvetlen előzményének tekinthető rajzok, szimbólumok barlangok falain, később kőtáblákon, illetve agyagtáblákon jelentek meg. Az első rögzített adatok meghatározott javak felsorolását tartalmazták megadva azok mennyiségi jellemzőit és a hozzátartozó mértékegységet is, mint az adatszerűség kiinduló, elsődleges kritériumait.

Az adatok továbbításának technikai feltételeit a papír, illetve papírjellegű írásfelületek és a hozzájuk tartozó írószerek megjelenése teremtette meg. Ezen túlmenően létrejöttek az adatok tárolásának, illetve sokszorosításának egyelőre kezdetleges, korlátozott, de mindenesetre bővülő, és a döntéshozatalt egyre hatékonyabban támogató feltételei. A kezdet a tekercs jellegű adatrögzítés volt, majd ezt követően a kézzel írott kódexek, könyvek, feljegyzések már lehetővé tették a könyvtárak, archívumok formájában az első, mennyiségi értelemben vett adatbázisok megjelenését. További fontos fejlődési fokozat volt a nyomtatás megjelenése és elterjedése, mely tömegessé tette az információhordozókat, könyveket, újságokat és az emberek közötti közvetlen üzenetváltás, hírek, adatok továbbításának lehetőségét, ezáltal az emberek mindennapi életének, így a döntéshozatali folyamatnak is alapelemévé tette az adatok és ismeretek megszerzését és felhasználását.

A XIX. század rohamos ipari fejlődésével párhuzamosan kifejlődött a hang- és képjelek alkalmazásának, felhasználásának, illetve továbbításának technológiája. Az alkalmazás és felhasználás azt jelenti, hogy megnövekedet, és fokozatos mennyiségi és minőségi fejlődésnek indult a hírek és adatok megszerzését szol-

gáló érzékelők rendszere. Ennek következtében jelentősen kibővült a hírek és adatok megszerzésének lehetősége, illetve a műszaki-technikai feltételek fejlődése következtében fokozódott a tartalmi pontosság, a precizitás és a valósághűség. A továbbítás technológiájának fejlődése nem csak a hírek, adatok a korábbiaknál jelentősen felgyorsult továbbítását, hanem a továbbítás megbízhatóságának fokozódását is elősegítette. Ezzel párhuzamosan fejlődtek az adathordozók, mindenekelőtt a hang- és képfelvételek technológiája, mely egyben elősegítette felhasználásuk hatékonyságának fokozását is. Ennek a fejlődési fokozatnak az előnyökkel párhuzamosan megnövekedtek a kockázati tényezői is. Ilyen kockázati tényező a továbbított adatok elfogása, a továbbítás megakadályozása, illetve az elfogott adatok manipulálása.

A műszaki-technológiai, tudományos fejlődés az elmúlt évtizedben eljutott a digitalizálódás és a miniatürizálódás szintjére, amely az egyidejűleg bekövetkező informatikai, elektronikai fejlődéssel, valamint a kibontakozó globalizálódással párhuzamosan megteremtette az adathálózatok elterjedésének, az azonos idejű érzékelésnek, adatszerzésnek és továbbításnak, illetve az adatbázisok elterjedésének és – gyakorlatilag – területi korlátoktól független használatának feltételeit.

Az Egyesült Államok katonai értelmező szótárát alapul véve az adatbázis az adatok felhasználói hozzáférésre és felhasználásra, műveletek végzésére alkalmassá tett strukturált, rendszerezett tárolása. Az adatbázis megjelenési formája lehet nyomtatott anyagok – könyvek, gyűjtők, okmányok, jegyzőkönyvek, stb. – gyűjteménye, illetve automatizált informatikai rendszerek adathordozóin tárolt adatok összessége.¹⁴

A történelmi fejlődés áttekintése képet ad arról, hogy az adat és az adathordozó egymással párhuzamosan fejlődött, bővült. Ebben a folyamatban az adathordozó fejlődése jelentős mértékben felhasználta, esetenként ösztönözte a műszaki-technológiai és tudományos vívmányok, találmányok eredményeit, és ezzel jelentősen hozzájárult az adatok érzékelésének, tartalmi bővülésének, megszerzésének, tárolásának, felhasználásának mindenirányú fejlődéséhez. Az adatokhoz történő hozzáférésnek, az adatok birtokba vételének két alapvető formája van.

Az adatgyűjtés, adatszerzés

Az adatgyűjtés a különböző adatbázisokban mindenki részére elérhető, megtalálható tartalom spontán, vagy meghatározott célú összegyűjtése tájékozódás, ismeretbővítés, vagy további céltudatos, célirányos tevékenység megalapozása

¹⁴ JP1-02, *Department of Defense Dictionary of Military and Associated Terms*; 8 November 2010. (Amended Through 15. April 2012.) p. 83.

céljából. Az adatgyűjtés kiinduló pontja és alapfeltétele a tartalmi érdeklődés mellett az adatbázisok használatának ismerete. Az adatbázisokban történő keresés alapvetően a tárgyra, témára, illetve a kulcsszavakra irányul.

Az adatszerzés felhasználja, alkalmazza az adatgyűjtést, mint módszert, de túllépi annak viszonylagos passzivitását, határát, és mint ilyen aktív, irányított, tervszerű, céltudatos tevékenység. Az adatszerzés túllépi a közvetlen hozzáférhetőség határát is, keresi, kutatja az adatokhoz történő hozzáférés egyéb módszereit, továbbá az adatok belső összefüggéseit, logikáját, mélyebb, sokoldalúbb felhasználhatóságának lehetőségeit. Az adatszerzést a döntéshozatalt támogató információszerző és feldolgozó szervek a politikai és katonai döntéshozó szervek feladat-meghatározása, információigénye¹⁵ alapján végzik. De az adatszerzés nem csak a döntéshozatalt támogató szervezetek privilégiuma. Adatszerzést folytatnak bűnügyi, biztonsági, igazságügyi intézmények, a tudományos kutatók és az oknyomozó újságírók, politikai, gazdasági, pénzügyi szervezetek is, valamint a társadalmi tevékenységek irányításában és végrehajtásában résztvevő állami és nem állami intézmények. Az adatszerzés irányultságát az határozza meg, hogy milyen feladat végrehajtását szolgálja. Pl. ugyanazt az adatforrást eltérő rendező elvek alapján közelíti meg, és használja a nemzetbiztonsági, illetve a bűnügyi adatszerzés.

Az információigények alapján meghatározott adatszerzés feladata a biztonság és a veszélyek differenciált értelmezésének megfelelően mindig valamilyen konkrét szakterület adatainak megszerzése. Az egyes szakterületek önálló, saját jól definiálható ismeretanyaggal, feladattal, a feladatok természetéből adódó módszer-rendszerrel és struktúrával rendelkeznek, ennek következtében a rájuk vonatkozó hír- és adatszerzés módszereinek ezekhez a kritériumokhoz kell alkalmazkodniuk.¹⁶ Az elmúlt 10-15 év során a kapcsolatok építése, az információk információs hálózatokon keresztüli elérhetősége, az információs hálózatok sokoldalú felhasználhatósága és így az információigény által meghatározott adatok megszerzése is szinte korlátlanra vált. Ugyancsak kibővültek, és a korábbiakkal szemben új tartalmat kaptak az emberi kapcsolatok, melyek megfelelő, szakmailag, tartalmilag meghatározott feltételek mellett értékes információ elemek forrásai lehetnek. Másképpen kifejezve, minden kapcsolatfelvétel egyúttal adatszerzési lehetőség is.

A megszerzett adatok értéke, haszna, felhasználhatósága alapvetően a megszerzésben és az értékelésben résztvevő állománynak az adott szakterületre vonatkozó, szakmai-tartalmi, módszertani felkészültségétől, szaktudásától, ismereteinek korszerűségétől, és nem a megszerzés konspiráltságának szintjétől

¹⁵ *Request for Information.*

¹⁶ *Dr. JÁVOR Endre ezredes: Gondolatok a nemzetbiztonsági szolgálatokkal kapcsolatos vitákról, FELDERÍTŐ SZEMLE, Budapest. VI. évfolyam 3. szám 2007. szeptember. p 116.*

függ.¹⁷ Pl. egy katonai információ feldolgozásához a „kézműves” szinten megszerzett gyakorlati, a tudományosan megalapozott oktatási rendszerben kapott elméleti, és a saját tevékenységben megélt gyakorlati tapasztalatok során kifejlesztett katonai ismeretekre, a katonai szemléletmódra van szükség.¹⁸ Ez egy olyan, szakmai és módszertani ismereteket feltételező és igénylő tevékenység, amit éppúgy nem lehet mással helyettesíteni, mint például a humán orvos munkáját az állatorvoséval és viszont. Ugyanez vonatkozik az adatszerzés többi szakterületére is. Csak akik ismerik az adott szakterület tartalmi és módszertani sajátosságait, azok tudják meghatározni, megtalálni az megszerzendő adatok forrását, a megszerzendő adatokra vonatkozó adekvát kérdéseket feltenni, a megszerzett adatokat a megszerzés szintjén elsődlegesen elemezni, értékelni és feldolgozni.

Az adat határozza meg, hogy a hír milyen tulajdonságokkal rendelkezik, mi az, ami jellemző rá, mi az, ami csak rá jellemző, illetve mi az, ami biztosan nem. A hírekhez köthető adatok lehetnek strukturáltak, és strukturálatlanok.

A strukturált adat mérhető, ellenőrizhető paraméterekkel – számszerűsített dimenziókkal, szabványosított mértékegységekkel – rendelkezik, és pontosan definiálja az adott ismerethez tartozó fizikai jellemzőket. Ezek mindenekelőtt a térbeli elhelyezkedésre, időtényezőkre, fizikai méretekre, működési feltételekre, képességekre, teljesítményre stb.-re vonatkoznak. A strukturált adatokat meghatározott rendező elvek alapján rendszerbe lehet foglalni, és műveleteket lehet velük végezni. A strukturált adatok előnye, hogy elősegíti, megkönnyíti speciális adatok kikeresését, megtalálását, a hozzáférhetőség biztonságának megőrzését, fenntartását. Ugyanakkor hátránya, hogy kiszámítható, modellezhető, fenntartása, működtetése költséges, a feldolgozás során elveszhetnek részelemek, melyek más összefüggésben, vagy egy későbbi felhasználás során fontosak lehetnek, a keresés során összetéveszthetők hasonló strukturájú információkkal.

A strukturálatlan adatok szöveges leírást, magyarázatot, értelmezést adnak a hírekhez, megvilágítják az előzményeket, az összefüggéseket és helyet adnak az alternatív lehetőségek megvizsgálásának, felmérésének is. A strukturálatlan adatokat beérkezésük sorrendjében egy általános rendeltetésű, felhasználási paramétereinek megfelelően még nem kategorizált adatok részére fenntartott tároló helyen tárolják. Ezek később meghatározott feldolgozás után bekerülhetnek a strukturált adatok kategóriájába, vagy mint egyenlőre nem hasznosítható „melléktermék”, maradnak strukturálatlan adatok. A strukturálatlan, tehát fel nem dolgozott adatok szöveges formában kerülnek tárolásra, a keresésük pedig a strukturált információk kereséséhez hasonlóan kereső programok segítségével történik.

¹⁷ U.o.p. 117

¹⁸ *A hadszíntér előkészítés elemzése, értékelése a hadszíntér elemeinek, funkcióik, egymáshoz való viszonyuk, ismerete nélkül elképzelhetetlen.*

A strukturálatlan adatok nem manipulálhatók, nem modellezhetők, fenntartásuk, működtetésük kevésbé költségigényes, nem vesztik el a részinformációkat, kevésbé áll fent az összetévesztés veszélye. Ugyanakkor a speciális adatok keresése, megtalálása nehezebb, a műveletek végzése pedig csak manuális formában végezhető el.

Ha sikerül egy, az információ igényrel összhangban levő hírt megszerezni, azonnal meg kell kezdeni a hírre vonatkozó adatok megszerzését. Az adat teremti meg a hír hitelességének, megbízhatóságának alapját. A hitelesség, megbízhatóság vizsgálata, megállapítása, ellenőrzése, összehasonlítása a hírek, adatok feldolgozásának folyamatában történik. Az adatfeldolgozás eredménye a döntéshozatal igényeinek kielégítését lehetővé tevő információ.

Az adatfeldolgozás

Az adatfeldolgozás a döntéshozatalt támogató információ vonatkozásában nem egyéb, mint a megszerzett és rendelkezésre álló hírek és adatok elemzése, értékelése, továbbá az információ igény által megfogalmazott szempontok alapján, a félreértésektől, esetleges megtévesztésektől amennyire lehet megtisztított, a döntéshozatalhoz használható információ létrehozása.

A megszerzett hírek és adatok valódi értéke az elemző, értékelő, feldolgozó folyamat eredményeképpen válik a döntéshozatal támogatására alkalmas információvá. A hírek és adatok megszerzésének eredménye, értéke, haszna az elemző, értékelő, feldolgozó munka eredményeképpen realizálódik, válik a döntéshozatal folyamatában használható ismeretté, tudássá. Habár korszerű körülmények között az adat- és információs technológia ezen a területen is egyre fontosabb szerepet játszik, az elemző, értékelő, feldolgozó munka alapja továbbra is a tudományos igényességgel végzett, az ember szellemi képességein, szakmai tudásán és ítélőképességén alapuló intellektuális folyamat marad.

A hírek és adatok megszerzésének a sokszínűsége azt eredményezi, hogy egy meghatározott célra irányuló információs igény kielégítésének a módszerei megsokszorozódtak. Pl. egy terrorista csoport működéséről, egy akció előkészítéséről adatokat lehet szerezni az úrben elhelyezett stacionárius eszközökkel, az elektronikai- és rádió-felderítő eszközökkel, a térségben állomásozó, vagy telepített felderítők útján, foglyok kihallgatásával, illetve nyílt források felhasználásával. Az így megszerzett híreket és adatokat egymástól függetlenül működő, egymástól eltérő rendező elvek alapján működő adatszerző szervek gyűjtik össze, egymástól esetenként időben és térben is elválasztva. Ennek következtében ezeket a híreket és adatokat mindenekelőtt egy ponton össze kell gyűjteni és koordinálni kell. A megszerzett hírek és adatok formája, természete, terjedelme és egyéb paraméterei a megszerzés módszerei függvényében eltérőek, és ebből a sokszínűségből egységes, és a döntéshozatal szempontjainak megfelelő információ létrehozása az elemző-értékelő munka feladata.

A modern kor és a jövő egyik jellegzetessége mindenféle - nyílt és titkos - hírek, adatok mennyiségének rohamos növekedése. Ennek egyik oka az emberiség egyre jobban kibontakozó anyagi és szellemi tevékenysége, illetve annak használatát, kutathatóságát, fejlesztését lehetővé tevő dokumentálás, archiválás igénye, szükségszerűsége. A másik ok az adatfeldolgozás és tárolás műszaki-technikai feltételeinek rohamos fejlődése, mely lehetővé tette a gyakorlatilag korlátlan mennyiségű hír, adat, információ dokumentálását, reprodukálását, kutatását, műveletek végzését és új további új információk előállítását. Ezt a mennyiséget papíralapon, nyomtatással már nem lehet feldolgozni, és olyan széles körben publikálni, mint az napjainkban már hétköznapi gyakorlat. A mennyiségi növekedéssel párhuzamosan egyre inkább differenciálódik, egyre sokoldalúbbá válik az információ tartalma, minősége.

Az információ döntéshozatalt támogató funkciója

A döntéshozatalt támogató információ alapja valamilyen esemény, tevékenység, melyet egy adott közösség, ország működése inspirál, igényel, mely egy adott közösség, ország érdekében történik, és egyidejűleg befolyásolja más országok, közösségek életét, politikáját. A történelem korábbi időszakaiban, gyakorlatilag a XX. század végéig a társadalmi tevékenységek, különösen a politika és a biztonság tervezése során az egyes országok, közösségek csak a saját érdekeikre koncentráltak, figyelmen kívül hagyták más országok közösségek érdekeit. Az események, tevékenységek megnyilvánulásai, következményei, hatása, illetve a megvalósítására vonatkozó döntés, a tervezés és végrehajtás, valamint a végrehajtás irányítása és a végrehajtásban résztvevő erők, eszközök testesítik meg azokat a híreket, adatokat, melyek megszerzésére az ellenérdekeltek, vagy rivális országok, közösségek törekedtek. Valójában, akik ebben a tevékenységben különösen tervező, irányító, vezető szinten részt vesznek, képezik azoknak a körét, akik az esemény, tevékenység vonatkozásában a legtöbb, legátfogóbb ismeretel, tudással, információval rendelkeznek.

Azok az országok, közösségek, amelyek érdekeik sérelmét feltételezve a számukra veszélyesnek ítélt eseményre, tevékenységre vonatkozó információ megszerzésére törekednek, akadályok, nehézségek egész sorával találják szembe magukat. Számolni kell pl. a hírek, adatok védelmére hozott intézkedésekkel, a megtévesztéssel, illetve a megszerzés során elkövetett hibákkal, pontatlanságokkal, az időtényezővel, az értelmezési problémákkal, vagy akár a kezelhetetlenségig nagytömegű, ellentmondásokkal teli információtömeggel. Ennek következtében számukra nagyon fontos, hogy a megszerzendő információt minél több forrás felhasználásával, a lehető legszélesebb alapon közelítsék meg és dolgozzák fel.

A társadalmi, tudományos, műszaki-technikai fejlődéssel párhuzamosan a felderítendő – politikai, katonai, diplomáciai, gazdasági, stb. – események, tevé-

kenységek egyre összetettebbé, egyre strukturáltabbá váltak. Ennek megfelelően fejlődtek az adott események, tevékenységek következményei, illetve mérhető, érzékelhető megnyilvánulásai, a rájuk vonatkozó hírek, adatok megszerzésének lehetőségei, és nehézségei. Mindenesetre a megszerzett hírek, adatok információ értékének mennyisége, minősége csak egy valamilyen arányú töredéke a teljes és valódi ismeretanyagának, illetve annak, amivel az események, tevékenységek végrehajtásában, irányításában résztvevők rendelkeznek.¹⁹

Az információhoz történő hozzáférés a történelem korai időszakaiban azon keveseknek volt a privilégiuma, akik rendelkeztek a hírek és adatok megszerzéséhez és különösképpen továbbításához szükséges – kapcsolati, technikai és pénzügyi - feltételekkel. Ebben az időszakban – mint arról már említés történt – maga a nyers hír volt az információ. Tekintettel a hírek és adatok megszerzésének nehézségeire a fő erőfeszítés iránya ezeknek a már említett nehézségeknek, akadályoknak a leküzdésére irányult, és megszerzett hírek, adatok feldolgozásának szükségessége bizonyos értelemben háttérbe szorult. Ez különösen akkor fordult elő, amikor a megszerzett hír, adat alátámasztotta, megerősítette az el-lenségkép alapján kialakult előítéleteket. A kezdeti tapasztalatok azonban azt is megtanították, hogy a nyers hírek, adatok nem elegendőek a döntéshozatalhoz. Ha egy, vagy számszerűen kevés hír, adat áll rendelkezésre, akkor a döntéshozók vagy nem tudnak dönteni, vagy elhamarkodott döntést hoznak. Ezt megelőzendő ki kellett dolgozni és meg kellett tanulni azokat az eljárásokat és módszereket, melyek egyrészt az egyes hírek, adatok hitelességének, valóságtartalmának vizsgálatát, megállapítását teszik lehetővé, másrészt a megszerzett hírek, adatok összehasonlítását, ellenőrzését, kritikus felülvizsgálatát, és ezen keresztül azok feldolgozását, a velük végzett műveletek szükségességét, fontosságát egyre inkább előtérbe helyezte. Ennek első lépése a hírek, adatok megszerzésének diverzifikálása, ami azt jelenti, hogy nem szabad megelégedni egy módszerrel, egy forrással. Korszerű körülmények között egy adott eseményre, tevékenységre vonatkozó hírek, adatok megszerzésére egyidejűleg, illetve egymást kiegészítve alkalmazni lehet pl. az emberi erővel végzett felderítést,²⁰ a nyíltforrású felderítést,²¹ a vezetékes és vezeték nélküli híradás adatforgalmának felderítését,²² az elektronikus rendszerek felderítését²³ is, illetve egyéb egyedi eljárásokat is. Ezt a módszert a nemzetközi szakirodalom „összforrású” hír- illetve adatszerzésnek nevezi.

¹⁹ Clausewitz írja klasszikus művében, hogy a - háborúra vonatkozó – hírek egy része ellentmondásos, nagy részük hamis, egy még nagyobb részük pedig bizonytalan. (Carl von Clausewitz: *Vom Kriege*. Rowohlt. München 1963 p. 48.)

²⁰ HUMNINT

²¹ OSINT

²² SIGINT

²³ IMINT

Mindaddig, ameddig a hírek, adatok megszerzése privilégium volt, addig igaz volt az a gyakran hangoztatott mondás, hogy az „információ hatalom”. Ahogy azonban bővült a társadalmi tevékenységek tartalma, hatása, az ismeretek, tapasztalatok feldolgozása iránti – tudományos – igény, illetve a tartalom rögzítésének, tárolásának, felhasználásának és továbbításának műszaki-technikai feltételei, úgy tágult azoknak az intézményeknek, szervezeteknek, társadalmi csoportoknak és egyéneknek a köre, akik hozzáférhettek a korábban elérhetetlen hírekhez, adatokhoz.²⁴ Az adathordozók és az adatbázisok körének kibővülése lehetővé tette az alapinformációkhoz²⁵ történő korlátlan hozzáférést is. A megváltozott feltételek egyik fontos kísérő jelensége, hogy a korábbi elzárkózással szemben egyre inkább a közlékenység, bizonyos értelemben a kitárulkozás kultusza bontakozott ki. Napjainkban már senki nem a hírek, adatok hiányáról beszél, megoldandó probléma a nagytömegű információ szelektálása, a fontossági szempontok felismerése.

Az információ általánosságban összeköti az embereket, a társadalom tagjait, alkotó elemeit egyrészt egymással, másrészt a társadalmi tevékenységekkel. Az információ teszi lehetővé, teszi élővé, működőképpé a társadalmi folyamatokat. Az információ a társadalom, a társadalmi folyamatok vérkeringése, tápláléka, éltető, életben tartó és a fejlődését lehetővé tevő eleme.

A döntéshozatalt támogató információ a társadalom létét, működését, biztonságát befolyásoló eseményeknek, folyamatoknak, tevékenységeknek, mint rendszernek a struktúrájára, tulajdonságaira vonatkozó ismeret, tudás összessége. Az információ megismerése a rendszer működése megismerésének, megértésének és hasznosításának, felhasználásának, vagy az általa okozott veszélyek, hátrányok felismerésének alapfeltétele.

Összefoglalva: politikai, biztonsági, katonai értelemben az információ:

- ismerethiányt, bizonytalanságot szüntet meg, vagy segít megszüntetni;
- a döntéshozatal – második - alapeleme; (első a célkitűzésből levezetett információ igény)
- hírek, adatok strukturált feldolgozásának eredménye;

A dokumentáció

A dokumentáció eredeti jelentése szerint hivatalos okirat, okmány, mely valamilyen viszonyrendszeren belül bizonyító erővel, jogosultsággal rendelkezik. Ilyen volt pl. az útlevel, amit az egyik ország hivatalosan kiadott állampolgárainak. Erről hitelt érdemlően értesítette az általa diplomáciailag elismert országokat, és

²⁴ Kibővült a hatalom birtokosainak, haszonélvezőinek köre.

²⁵ Alapinformáció – a meglevő és elérhető információk összessége.

kérte őket, hogy fogadják el az általa kiadott okmányt. A rendszer működésének feltétele a kölcsönösség, azaz az országok kölcsönösen elismerték egymás útleveleit, egyéb hivatalos okmányait, pl. jogosítványt, házassági okmányokat, stb. A lényeg, hogy bizonyítható legyen a dokumentum kiállítójának felhatalmazása, jogosultsága. Ezen a ponton azonban kibővül a dokumentáció értelmezése. Ebbe a kategóriába tartoznak egy ország hivatalos szervei által előállított politikai, katonai, biztonsági döntéshozatali rendszerében keletkezett, szakemberek által előállított okmányok, tervek, koncepciók, végrehajtási utasítások, térképek, stb. Ugyancsak ebbe a kategóriába tartoznak a bírósági, ügyészségi és jogi relevanciájú anyagok, illetve tudományos intézmények, szervek hivatalos kiadványai, kutatási anyagai. Ebből levezethető, hogy a felhatalmazáson túlmenően a dokumentáció fontos kritériuma a tartalmi, szakmai hitelessége, valóságtartalma.

A dokumentáció klasszikus formája a papíralapú okmány. A fejlődés következő állomása a tárgyi dokumentumok megjelenése volt. Ezen a fokon egy tárgy, pl. egy fegyveralkatrész, vagy a képi, illetve audió adathordozók már a dokumentációk egy új kategóriáját jelenítették meg. Az információs korszak új jelensége, hogy a papíralapú dokumentumok helyét egyre inkább átveszik az infokommunikációs adattárolók, vagy más, automatikus előállítású, hálózati rendszerek által ellenőrizhető és működtethető, praktikusán használható eszközök. Ugyanakkor napjainkban dokumentáció minden olyan forrás, melyet bármilyen – mindenképp előtti elektronikus, hálózati - adatbázisból lehet megszerezni.

A dokumentáció rendeltetése hiteles ismertek közvetítése további felhasználás céljából. Ennek megfelelően a dokumentáció alkalmazkodik az egyes szakterületek szabályaihoz, struktúrájához. A politika és a biztonság területén ide tartoznak a stratégiák, tárgyalási jegyzőkönyvek, szerződések. Katonai téren dokumentáció pl. egy mozgósítási terv, egy fegyverrendszer beszerzési pályázata, egy tervezett gyakorlat előkészítési okmányai. Tudományos területen dokumentáció egy kutatási jelentés, egy szakdolgozat, egy szakmai folyóirat. A gazdasági, ipari, pénzügyi szféra dokumentációi közé tartoznak a költségvetési tervek, üzleti tervek, ajánlatok, szerződések, számlák, tárgyalási és egyéb jegyzőkönyvek, stb.. Ezek a dokumentációk jelentős mennyiségben tartalmazzák a döntéshozatal során felhasználható adatot, információvá feldolgozható tudást, ismeretet.

A dokumentáció kezelésére a kiadója, készítője tulajdonosa szabályokat határoz meg. A szakterület, fontosság, az állami, intézményi hierarchiában elfoglalt hely függvényében meg lehet határozni azoknak az intézményeknek, funkcióknak, személyeknek a körét, akik címzettjei a dokumentációnak, illetve hozzáférhetnek az adott dokumentációhoz. További előírások szabályozhatják az érvényesség kritériumait, a kiegészítő és kíséző dokumentációkat, hivatkozásokat, illetve érvényességének korlátait, határait. A dokumentációkat kiadójának szándéka szerint minősíteni lehet, ami országonként eltérő formában, de a titkosság különböző fokait jelenti meg, névre, beosztásra korlátozott zártkörűen terjesz-

tett, a szigorúan titkos, bizalmas anyagokon keresztül egészen a korlátozatlan, nyílt terjesztésű kiadványokig.

A dokumentáció tehát hiteles, valós, felhatalmazott, jogosultsággal rendelkező forrásból származó, tartalmi, szakmai szempontból releváns tartalmú híreket, adatokat, rész- vagy teljes információkat tartalmazó anyag, mely lehetővé teszi az adott szakterülettel foglalkozó szervek, intézmények részére, az adatbázisokból, vagy más egyéb úton megszerzett dokumentációk anyagának ellenőrzését, továbbfejlesztését, valamint saját igényeknek megfelelő új információk kidolgozását.

Nemzetközi kitekintés

Hiányos maradna a gondolatmenet, ha nem vetnénk egy pillantást a nemzetközi szakirodalomban a „hírszerzés” értelmezésével kapcsolatos megfogalmazásokra. Ha nyilvánvalóan más okokból is, csakúgy, mint napjainkban, már a XIX. században is a magyar szakkifejezések jelentős része, különösen a biztonság, a katonai és védelmi területeken idegen nyelvből történő fordítás eredményeképpen született. Ebbe a kategóriába tartozik a „hírszerzés” is, mely nagyfokú hasonlóságot mutat a napjainkban is használt német „Nachrichtendienst” kifejezéssel. Ebben a kifejezésben a „Nachrichten” a hír, a „Dienst” pedig a szolgálat megfelelője, és arra utal, hogy eredeti funkciója a hírek továbbítása volt, de nem utal a tartalmi vonatkozásokra, ismertre, tudásra.

Ennél kifejezőbb az angol nyelvű „Intelligence” kifejezés. Ennek széleskörű értelmezési tartománya – a teljesség igénye nélkül – a szervezett információ-szerző tevékenységen, az ezzel a tevékenységgel foglalkozó intézmény, illetve az információszerzés eredménye megjelölésén²⁶ túlmenően felöleli a megismerést, a megértést, a problémamegoldó gondolkodást,²⁷ valamint az öröklött és tanult emberi tulajdonságok, képességek, ismeretek olyan továbbfejlesztett megnyilvánulását, mely egy ismeretlen, váratlan helyzethez történő magasabb fokú, adekvát, célirányos, hatékony alkalmazkodást tesz lehetővé. Ezen a logikán elindulva eljutunk az ismeret, a tudás, az információ szerepének, fontosságának felismeréséhez, majd ezen keresztül pedig az ismeret, a tudás és az információ megszerzésének, feldolgozásának funkciójáig, illetve ahhoz a képességhez, mely megteremti a döntéshozatal támogatásának feltételeit. Következésképpen ez a kifejezés teljes mértékben lefedi, tartalmazza mindazokat a kritériumokat, melyeket a döntéshozatalt támogató információszerzés, mint funkcionális tevékenység megtestesít.

²⁶ JP1-02, *Department of Defense Dictionary of Military and Associated Terms*; 8. November 2010. (Amended Through 15. April 2012.) p. 164.

²⁷ *The English Illustrated Dictionary*. AWARD Publications London 1986. p. 436

Összehasonlítva a magyar és az angol kifejezést, látható, hogy a „hírszerzés” tartalmazza az angol kifejezés első két elemét, a tevékenységet és az intézményt, de nem tartalmazza a harmadik, a tudásra, ismeretre, tehát a tartalmi összefüggésekre utaló elemet. Ilyen körülmények között természetes igény és szükséglet a fogalom továbbfejlesztésére irányuló szándék.

Befejező gondolatok

Lépést tartani a fejlődéssel annyit jelent, mint alkalmazkodni a megváltozott feltételekhez, és körülményekhez. A fejlődés tendenciája azt mutatja, hogy míg a hidegháborút megelőző, az ellenségképre, előítéletekre épülő hírszerzés központi fogalma a titkos módszerek alkalmazásával megszerzett titok volt, korszerű körülmények között a központi fogalom az ismeretet, tudást tartalmazó információ. A belső, tartalmi folyamatokkal párhuzamosan változik, fejlődik a fogalmi apparátus is. Vajon megjeleníti-e, képviseli-e a régi fogalmi apparátus a változás tendenciáit? Erre a problémára keres választ ez az írás azzal a nem titkolt szándékkal, hogy hozzájáruljon egyrészt a közvélemény által misztikusnak tartott szakterület jobb megértéséhez, másrészt a szakterületen belül feltétlenül szükséges szemléletváltáshoz.

Megszoktuk, axiomatikusan használni a „hírszerzés”-t, mint fogalmat, de a mögötte levő tartalom értelmezés kérdése. Első megközelítésben azt lehet mondani, hogy azt az időszakot képviseli, amikor a még maga a megszerzett nyers hír volt a szinte egyetlen információ, amire a döntéshozatal egyáltalán hagyatkozhatott. Habár a megszokásokon, hagyományokon nagyon nehéz változtatni, a tudományos-technikai fejlődés teremtette feltételek mellett természetes követelmény a fogalom tisztázására irányuló szándék. Az már első megközelítésben is látható, hogy a „hírszerzés” szó két eleme, a „hír” és a „szerzés” a döntéshozatal támogató folyamatban már nem tölti be azt a szerepet, ami az eredeti értelmezés szerint neki tulajdonítható volt.

Napjainkban a "hírszerzés" központi fogalma nem a "titok", hanem a tudás, az ismeret. Nem titkos módszerekkel megszerzett titkokra van szükség a döntéshozatalhoz, hanem a döntéshozatal igényei alapján megfogalmazott ismeret és tudás elemeire. Nem elegendő a csekély számú, titkos módszerekkel megszerzhető hír és adat, mikor az ismeretet és tudást megalapozó hírek és adatok a tudományos igényű módszerek és eszközök alkalmazásával szerezhetőek meg. Korszerű viszonyok között az adekvát döntéshozatal az elemzett, értékelt, alternatív választási lehetőséget biztosító ismeretre, tudásra épül, ami magába foglalja a különböző emberi és technikai adatszerző rendszerek által megszerzett adatok célirányos feldolgozását.

A nemzetbiztonsági tevékenységnek a társadalmon belül kettős funkciója volt és van. Egyrészt van egy hatalmi, másrészt egy szolgáltató funkciója melyek közül a hidegháborút megelőző időszakban a hatalmi funkció volt domináns, a

szolgáltató funkció szinte észrevétlen, érzékelhetetlen volt. A nemzetbiztonsági tevékenység működtető eleme napjainkban tehát nem a hír, hanem a hírek, adatok feldolgozása, elemzése, értékelése útján az információ igény által meghatározott feladatoknak megfelelően feldolgozott létrehozott, tudást, ismeretet tartalmazó információ, melyet az erre a feladat végrehajtására létrehozott szervezetek, intézmények, szolgálatok, mint kész terméket a döntéshozók rendelkezésére bocsájtanak, tehát szolgáltatást végeznek. A fejlődés és a szükséges szemléletváltás egyik fontos eleme annak felismerése és tudomásul vétele, hogy a hatalmi funkcióval szemben tendenciájában előtérbe kerül a nemzetbiztonsági tevékenység szolgáltató funkciója.

Az információ valóságtartalma, felhasználhatósága, minősége az elemző, értékelő, feldolgozó munka minőségének függvénye. Ami egyrészt azt jelenti, hogy a döntéshozatalt információval történő támogató tevékenység valós tartalmát kifejező – jövőbeni használatra javasolt - megnevezés a korábban használt "hírszerzés" helyett az "információszerzés", másrészt kifejezi azt a szemléleti változást, mely a módszer-centrikus szemlélettel szemben a tartalom-centrikus szemléletet testesíti meg.²⁸

Felhasznált irodalom:

- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. (<http://mkogy.jogtar.hu/?page=show&docid=99500125.TV>; letöltve: 2016.01.23.)
- 2014. évi CIX. törvény a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény, valamint egyes törvényeknek a nemzetbiztonsági ellenőrzéssel összefüggő módosításáról. <http://mkogy.jogtar.hu/?page=show&docid=a1400109.TV> letöltve: 2016.01.23.
- Carl von CLAUSEWITZ: Vom Kriege. Rowohlt. München 1963.
- CSÁNYI Vilmos: Íme, az ember. A humánetológus szemével. Libri. 2015. Budapest.
- Dr. JÁVOR Endre ezredes: Gondolatok a nemzetbiztonsági szolgálatokkal kapcsolatos vitákról, FELDERÍTŐ SZEMLE, Budapest, VI. évfolyam 3. szám 2007. szeptember. P. 114-119.
- Dr. NAGY Péter: Virtuális diplomácia – mítosz vagy valóság (A "rég" és a "modern" diplomácia) <http://www.inco.hu/inco7/infopol/cikk1h.htm> (Letöltve: 2012.06.20.)

²⁸ Ez a gondolatmenet összhangban van a Nemzetbiztonsági Törvényben és módosításaiban leírt feladat meghatározásokkal, és az azokat megjelenítő szakkifejezésekkel.

- FM 3-05.102; ARMY SPECIAL OPERATIONS FORCES INTELLIGENCE Headquarters, Department of the Army July 2001 (SUNGUO – INT)
- Gregory F. Treverton: The Next Steps in Reshaping Intelligence - CHAPTER TWO Where Reform Stands p 3-15; Published 2005 by the RAND Corporation.
- Hadtudományi Lexikon. Magyar Hadtudományi Társaság. Budapest 1995.
- Handbook on Long Term Defence Planning
[http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-069///TR-069-\\$\\$TOC.pdf](http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-069///TR-069-$$TOC.pdf) (Letöltve: 2012.06.20.)
- Intelligence Analysis: Behavioral and Social Scientific Foundations - PART IV: ORGANIZATIONS (Baruch Fischhoff and Cherie Chauvin, Editors) THE NATIONAL ACADEMIC PRESS Washington, D.C. www.nap.edu. 2011. Letöltve: 2104.07.21.
- Intelligence Analysis for Internet Security
<http://www.cert.org/archive/html/Analysis10a.html> (Letöltve: 2012.06.20.)
- Janusz Piekalkiewicz: Die Weltgeschichte der Spionage, Südwest Verlag GmbH & CO. KG 1988 München.
- John W. Bodnar: Warning Analysis for the Information Age: Rethinking the Intelligence Process. Chapters 6 & 7. The Joint Military Intelligence College WASHINGTON, DC December 2003.
- JP1-02, Department of Defense Dictionary of Military and Associated Terms; 8 November 2010 (Amended Through 15 April 2012)
- Kalla Gábor: Az írásbeliség kezdetei és a korai írásbeliség társadalmi beágyazottsága, (http://gepeskonyv.btk.elte.hu/adatok/Okor-kelet/Okori.es.keleti.nyelvek.es.irasok/index.asp_id=159) (Letöltve: 2012.07.20)
- Making Intelligence Smarter
<http://www.fas.org/irp/cfr.html> (Letöltve: 2012.06.20.)
- NATO Open Source Intelligence Handbook. November 2001, http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf (Letöltve: 2012.06.20.)
- New Craft for Peacekeeping Intelligence
www.oss.net/.../Peacekeeping%20Intelligence%20Article%201.3.doc (Letöltve: 2015.01.20.)
- Robert David STEELE Vivas: Fixing the White House & National Intelligence
http://www.oss.net/dynamaster/file_archive/090105/442c15938640a86ca8113c4db296145d/Fixing%20WH%20and%20IC%20Steele%202009%201.5%20PDF.pdf (Letöltve: 2103.05.05.)
- STRATEGIC INTELLIGENCE AND ANALYSIS; Selected Writings by Don McDOWELL

http://www.intstudycen.com/docs/stra_select_writ_2000.pdf (Letöltve:
2010.08.17.)

- Szentírás. Mózes öt könyve. Szerk. Dr. Hertz J.H. Második kiadás. Akadémiai Kiadó Budapest 1984.

Practical Issues of IT Security Incident Handling in Market Environment and in Public Administration

Gábor Sági¹

Abstract:

Without the knowledge of events taking place in IT systems and their analysis from security's point of view, the organizations cannot ensure the business and legal expectations and adequacy. The author in this article introduces the criteria needed to realize efficient security event and incident handling, including technical, processual and legal aspects.

Keywords: incident handling, security operation center

Absztrakt:

Az informatikai rendszerekben zajló események ismerete, biztonsági szempontból történő elemzése nélkül a szervezetek nem tudják biztosítani az üzleti és jogszabályi elvárásokat, megfeleléseket. A szerző jelen cikkében bemutatja milyen feltételek szükségesek a hatékony biztonsági eseménykezelés megvalósítása érdekében, legyen szó az eseménykezelés technikai, folyamat vagy jogi aspektusáról.

Kulcsszavak: incidens kezelés, biztonsági felügyeleti központ

¹ PhD student of NKE, e-mail: gabor.sagi@yahoo.com, ORCID identifying number: 0000-0002-4473-0895

Review

All the actors of the market and society, the state's institutions, educational institutions are forced to introduce newer and newer services as our age requires to serve their clients better and more efficiently. The more complex requirements, the shortening of development lifecycles and the lack of available financial sources are bound to carry possible failures caused by the inadequacy of planning or implementation. Because of the more complex structure of systems the number of visible or less visible failures are increasing. Contrary to the errors in business processes which are noticed in a short time, the errors in operation, security insufficiencies come to light in connection with an incident such as the slowing down or the shutting down of the system or - in case of security insufficiencies – the unauthorized modification or disclosure of data handled in the system. Failures in business processes usually can be avoided by thorough testing, those in operation can be avoided by deliberate planning and by the selection of an adequate configuration, but the avoidance of security insufficiencies can only be ensured limitedly because of the high number of system components, the errors within, and because of unknown vulnerabilities. It is especially important to the secure operation of the system that the improper functioning comes to light i.e. the alert of the loss of the system's and the stored data's integrity, confidentiality and availability reaches the assigned (IT security and/or operational) division. The loss of availability is usually easily noticeable, the loss of integrity and confidentiality is not so spectacular, in a lot of cases during the monitoring of the system's parameters they may stay invisible. To make these security events visible, it is essential to operate sufficient security systems and processes.

Mostly in such a large enterprise environment where numerous IT systems with different purposes operate, the effective information security can barely be realized without a security monitoring center which contains a central security system, the human resource operating it and the properly operating processes. In accordance with available resources and depending on the maturity of the organization, security operation can use different technological solutions, and depending on the organizational culture, can ensure the operation of the activity in frames of different organizational solutions. In general, the applied technological solutions, the legal options, the organizational frames and the organization's maturity define the quality and the quantity of the processes used during the security operation.

National Regulation

In case of critical information infrastructures important from the state's, the market's, the society's and defense's points of view Act No. CLXVI. of 2012. on the identification, designation and protection of critical infrastructures and facilities², and Act No. L. of 2013. on the electronic information security of the government and local governments (hereinafter: lbtv.)³ and their implementing regulations contain several rules in order to protect electronic information systems. The requirements and activity related to security events, or with international terminology: incident handling, are defined in the implementation regulations of lbtv. [Regulation of the Ministry of Interior No. 41/2015 (VII. 15.) on the technological security, the secure informational devices, products and the requirements of classification to security category and security level defined in Act No. L. of 2013 on the electronic information security of the government and local governments (hereinafter: Reg. No. 41.)⁴, as well as in Regulation of the Government No. 185/2015. (VII. 13.) on the governmental incident handling center and its functions and authority, and on the rules of security incident handling, the security incident's technical investigation and on the carrying out of the vulnerability testing process (hereinafter Reg. No. 185.)⁵]. While Reg. No. 185. contains the rules of notifying the incident handling center of security incidents and the investigation of said incidents, Reg. No. 41. contains requirements related to the security classification of the system for organizations operating (using and operating) electronic information systems themselves.

² Act No. CLXVI. of 2012. on the identification, designation and protection of critical infrastructures and facilities http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (downloaded: 2017.06.04)

³Act No. Act L. of 2013. on the electronic information security of the government and local governments http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (downloaded: 2017.06.04)

⁴ Regulation of the Ministry of Interior No. 41/2015 (VII. 15.) on the technological security, the secure informational devices, products and the requirements of classification to security category and security level defined in Act No. L. of 2013 on the electronic information security of the government and local governments
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (downloaded: 2017.06.04)

⁵ Regulation of the Government No. 185/2015. (VII. 13.) on the governmental incident handling center and its functions and authority, and on the rules of security incident handling, the security incident's technical investigation and on the carrying out of the vulnerability testing process
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm (downloaded: 2017.06.04)

In Reg. No. 41. the expectations of logging activity at the lowest security level appear⁶, but the requirement of security incident handling appear only in case of electronic information systems at least at security level 3, though the regulation gives few guidelines to what concrete technological content is enough to meet certain requirements.

Several national works are available on the possible processes of incident handling, on the participants, their activity and their responsibilities, but the technical literature is still in debt with works on the formation of supervisory competency, the technical competency necessary to operate processes.

International excursion

Incident handling on an international level has a greater past than the national, that is why the available literature is more extensive. From the available literature „*Computer Security Incident Handling Guide special Publication*”⁷ published as No. 800-61 in 2012 by NIST which describes in detail the elements of incident handling, the process and the communication between the participants is outstanding. From the NIST’s Publication No. 800-61’s different point of view, partly expanding its content and complementing it with newer but nonetheless important details for the formation, operation and maintenance of a new security center MITRE published the „*Ten Strategies of a World-Class Cybersecurity Operations Center*”⁸ and Cisco Press published the „*Building, Operating, and Maintaining Your SOC*”⁹, and many other, shorter works can be read on particular subfields from which the works published by SANS, Ernst & Young, Paladion and Gartner are outstanding.

Competencies of the security operation center

To operate an effective security supervision, numerous competencies are necessary, but which these competencies are, appear differently in different works.

⁶ SÁGI, Gábor: *Informatikai rendszerek naplózása (Nemzetbiztonsági Szemle MMXVII/I,* http://uni-nke.hu/uploads/media_items/sagi-gabor-az-informatikai-rendszerek-naplozasa.original.pdf (downloaded: 2017.06.04)

⁷ NIST 800-61 *Computer Security Incident Handling Guide Special Publication Revision 2* <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (downloaded: 2017.06.04)

⁸ MITRE Carson Zimmerman: *Ten Strategies of a World-Class Cybersecurity Operations Center* <https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf> (downloaded: 2017.06.04)

⁹ Joseph MUNIZ, Gary MCINTYRE, Nadhem ALFARDAN: *Building, Operating, and Maintaining Your SOC* CISCO Press 2016 ISBN-13: 978-0-13-405201-4

However, different literature works agree that these activities can be divided into three categories¹⁰:

- Preventive: during prevention such activities shall be done that make it impossible for the dangerous event to occur. Preventive measure is for example the content filtering of e-mails, which prevents the infiltration of harmful codes through mailing.
- Detective: during detection, you try to notice the attack or damage in progress as soon as possible, then you try to eliminate it before any critical damage is done. For instance, the use of an IDS¹¹ system alerts you of suspicious packets. Based on the detection you can perform other activities.
- Corrective: corrective measures decrease or eliminate the damage done by an event. Corrective measure is for instance the restoration of the system from a save, as well as having an insurance that provides cover in case of damage.

However, countless competencies can appear in the three groups of activities which are – in my opinion – essential to the effective operation:

- real time detection: notifications on communication channels (telephone, e-mail) or the detection of alerts coming from business/supervision/monitoring systems
- analysis of incidents, response and mitigation: the collection, analysis of information related to real time detection, the giving of possible response and mitigation to the incident
- Threat intelligence information management: the collection and analysis of technical, tactical, strategic information coming from external sources and the forwarding of relevant information to the divisions concerned (e.g.: forwarding vulnerability information to the IT operation division, forwarding operative information related to new attack techniques to IT management, forwarding strategic information to senior management level). Sharing threat intelligence information (e. g. on new attack forms, on new IoCs¹²) revealed inside the organization with other organizations.
- handling artifacts: the collection of evidence emerged during an incident and their storages in an adequate way (such as making a bit-by-bit copy¹³) and the investigation of activity (e.g. the analysis of malware, analysis of network traffic, analysis of endpoint activity,

¹⁰ MUHA Lajos: *Útmutató az informatikai biztonság megvalósítására önkormányzatok számára* http://www.kormanyhivatal.hu/download/0/1a/00000/it_biztonsag_onkormanyzatok_nak.doc (downloaded: 2017.06.01)

¹¹ IDS: intrusion detection system

¹² IoC: Indicator of Compromise, e.g. attacker IP addresses, suspicious file hash)

¹³ bit-by-bit copy: create an exact, bit stream copy of the original storage medium

- the maintenance, operation and development of the operation center: the performance of daily operational tasks, the fitting to the constantly changing IT environment, the incorporation of vulnerability information, and the incorporation of experiences collected during incident investigation that are essential to the effective supervision, which can be complemented even with the use of individually developed solutions
- the support of compliance tests and audits
- the support of inner fraud reconnaissance and investigation

In an organization, several competencies can be developed, although which are closely related to the organization's security operation system do not necessarily belong to the operation center, even though they are essential from the secure operation's point of view:

- discovery and management of vulnerabilities: the mapping of vulnerability of devices in the network infrastructure ad-hoc or periodically, the revelation of the real threat of vulnerabilities (e.g. if the system is not accessible from the outside according to the network map, the handling of the vulnerability can happen with a lower priority), the following of the vulnerabilities' reparations
- operation of border protection systems: the operation and configuration of the organization's border protection devices (firewall, router, proxy)
- penetration testing: putting systems operated by the organization into operation or the security testing of a system development before put into operation, and periodically in order to ensure that the system cannot be hacked even with special knowledge and devices
- security testing: the security testing of newly introduced functions and devices
- consultation: support in information security issues during the development systems
- awareness training: making materials for general and information security education related to security incidents, providing and organizing awareness trainings, and measuring the information security of employees (e.g. the willingness to open spams "created" by the security division, the handling of "accidentally" lost devices),
- media relations: communicating the daily course of business and security incidents

Depending on the information security involvement of the organization, the available resources and last but not least the organization's traditions, some competencies does not appear inside the organization, or if they do appear, it is not sure that they are under the operation of information security division. Based on my experience, in a lot of cases the network division is responsible for the operation of border protection devices, or for example security testing (involving penetration testing as well) is done by a dedicated testing group, the

other listed competencies can usually be found at other departments of the organization.

The condition of the security operation center's operation

To perform the tasks assigned to the security operation center all necessary conditions for its operation should be provided together. The lack of these conditions or reduced performance can significantly influence the quality of the incident handling competence.

- data, information providing
 - Data created in IT systems (e.g. security devices, endpoints, servers, applications) that are relevant from security's point of view have to be sent to the operation center for processing. These data can be descriptions of activities carried out on a computer (logs) or alerts of security systems. The task of the systems supporting the operation center is to process these data and notify the incident handlers of the security event's detection if necessary.
 - The relevant data from security's point of view related to IT systems (e.g. functions of systems, their locations, risks of systems, information on their vulnerability, data of the users). These data can improve the classification of incidents detected, the definition of the incident handling's priority, fasten the response for a security event significantly and can make the analytical activity easier.
 - Vulnerability information from external sources (e.g. CERT¹⁴, TI¹⁵ providers). Information from others' analyses of events can help effectively to protect an organization's information systems and carrying out preventive activity.
- operating processes
 - With the help of processes related to preventing incidents (e.g. awareness trainings, setting IoCs) the organization can be capable of preventing or stopping attacks at an early stage, and thus ensuring the secure operation of the organization.
 - Processes related to the identification and analysis of incidents ensure that with the automatic or manual investigation of data generated in information systems, those events can be identified

¹⁴ CERT: Computer Emergency Response Team

¹⁵ TI provider: threat intelligence provide (provide e.g. harmful IP's, domains, suspicious file hash)

- that have a malicious effect on the secure operation of an information system.
- Processes related to incident handling help the activity of incident handlers by ensuring workflow-based incident handling depending on the system's competencies even with automatic carrying out of activities (e.g. automatic sending of suspicious files to a behavior-based analysis system), sending the specifics of a harmful activity to the protection systems depending on the result of a given investigation (e.g. sending to the firewall and blocking automatically the IP address related to harmful traffic), and providing reporting competency.
 - With processes after closing the incident investigation (e.g. implementing experience, targeted awareness-raising) ensuring that the experience gained during security events are built in the daily work, those involved get information on preventing, noticing and handling attacks with similar specifics.
 - technical conditions
 - The security operation center must be evolved in a way that it would be suitable for continuous work and in case of a more serious security incident, it would be suitable for supporting more people's (usually leaders') effective work, for ensuring a war-room kind of operation. It is advisable to build the office in a way that complies with the highest ergonomic requirements (because of the continuous and in case of an incident, work under stress).
 - A complete IT environment – possibly independent from the company's infrastructure - has to be provided to the data sent to the operation center and to ensure the operation of processes for data analysis. It is advisable for the whole infrastructure to be independent (e.g. individually operated network segment, serves, communication channels).
 - providing personnel
 - For incident handling the personnel with adequate knowledge shall be provided. While for the detection and initial basic analyses of a security event an operator with a lower level of knowledge but with higher tolerance of monotony is suitable enough, for operating the analytical, engineering and hunter activities creative experts with a higher level of knowledge are needed. In a well put-together analytical team, an expert on every IT system can be found (e.g. Windows, Linux, network and database expert, malware analyst).

- o The employees operating the devices (hardware, software, network) which ensure the operation of the incident handling center must have experience with the operation and configuration of the devices used.

The structure and connections of the security operation system

In the previous chapters it was introduced what kind of competencies a security operation center can have and which conditions are needed to ensure these competencies. However, the existence of these competencies is not enough on its own to sustain the operation function, and to make the activity operable, these parts should be integrated with one another. This integrated approach is presented by the model published by Gartner¹⁶. (Figure 1.)



1. Figure - Gartner „Innovation Tech Insight for Security Operations, Analytics and Reporting”, 2015

The support of the incident handling process

¹⁶ Oliver Rochford, Paul E. Proctor: Innovation Tech Insight for Security Operations, Analytics and Reporting <https://www.gartner.com/doc/3166239/innovation-tech-insight-security-operations> (letöltve: 2017.06.02)

The most important part of the security operation center is the Security Operations Analytics & Reporting (SOAR) system, where the information generated in the relating systems appear to find out whether an event is indeed a security event and if so, to make its scope, effect, priority and the circle of those who should be involved in the incident handling definable, support the incident handling processes and, during the closing of an incident, to ensure the reporting of data gathered during the incident according to uniform principles and the sending of the report to the concerned parties.

The operators can get alerts from source systems in the SOAR, they can start the incident handling processes from here, the analysts can start the incident analysis from here or in case of suspicion, the hunting activity.

The visibility of a security event – data sources

The data generated in IT systems can arrive from multiple sources and in multiple ways. One of the most important element from the effectiveness of the security operation's point of view is the processing and analysis of logs and alerts of events occurred in different source systems (servers, work stations, network and other security devices), which are usually done by a central security information and event management system (SIEM). The log collection can be complemented with netflow and packet collections as well. It is the task of the SIEM system to receive and analyze technical threat intelligence information from external sources. Usually built in the SIEM systems, above the log collection and analysis function these systems are able to the correlation and statistical based analysis of data gathered, which ensures that the visibly not connected events are revealed.

One of the possible methods of recognition, primarily of security events with unidentified IoCs is the surveillance and analysis of endpoints' activity. Depending on the capability of the endpoint detection and response (EDR), above the recognition of signature-based attacks they are able to recognize unknown patterns of behavior, to evaluate the security risks of different activities and to find connection between events so as to alert to suspicious activities. The EDR systems beyond the surveillance of activity on computers provide the opportunity to download important objects to the analysis of running files, data in memory etc. from the device. The modern EDR systems are able to take automatic actions as well as manual ones to prevent from harmful activities on the devices connected to the network, with the containment of running applications, processes and disconnecting the device from the network.

Over the last few years the user and/or entry behavior analytics (UEBA) has been widely spreading, which identifies which activities differ from the "usual" activity from the activities in a system and/or from network traffic that may as well imply harmful activity. While a few years ago these products were intro-

duced to the market as independent products, nowadays – thanks to the acquisitions – this function has become an integral part of SIEM and other defense systems.

In order to collect and analyze traces of an occurred security incident, forensics equipment is used, which collects the traces of a security event from source systems such as data on hard drives, logs, network traffic and package data. The purpose of collecting is partly to support investigation and partly to support an occasional official or inner investigation with evidence.

Other information sources related to event handling

An organization – depending on its maturity – usually operates an Information Security Management System (hereinafter: ISMS), whose IT support can use a so-called GRC (Governance, Risk, Compliance) system, which may provide data from resources (e.g. services, systems, infrastructure's elements, human etc.) in the enterprise for the operation center and the risk data related to the resources to make it possible to set a priority during security event handling and for the analyzer to gain information important from the analysis' point of view as soon as possible.

In the information system operated by an organization, the existing and known vulnerabilities have a special importance because these points can easily be targets to an attack. At the same time, not all of these vulnerabilities mean an exploitable point of attack, though to define the possible involvement, the knowledge of network information is absolutely necessary beside vulnerability information. The important information for an incident handler are for example: in case of an alert coming from an IDS system, whether the initialization of an incident handling procedure is necessary, as the attack is against a system which is not vulnerable, or the target of the attack is inaccessible from the attacked network segment.

Information on change coming from the IT systems' patch management system partly helps the preparation of the SIEM, the central operation system for the change with configuring correlations, alerts and event handling procedures, and partly the false alerts caused by the different operation as a result of the system's change can be avoided.

The relations system of incident handling

Related to incident investigations and alerts, the incident handlers may initialize such changes that they cannot implement because of the lack of accessibility to the IT systems. These requests are advised to be initialized through ticketing (e.g. ServiceDesk) operated by the organization, where the incident handler can receive feedback on the status of the request from.

Even though the figure of Gartner does not include the sharing of threat intelligence, in my opinion it is an important part of the incident handling procedure. In case of larger organizations, the disclosure of non-classified information can be regarded as a social engagement, because in this way this organization may contribute to the formation of a more secure information society.

Security operation as a service

Mostly small and medium sized organizations – because of the lack of resources – cannot operate an individual information security event handling division, cannot evolve an effective and continuously working incident reaction competency. The situation is similar to those organizations that are legally obliged to use a central IT and electronic provider as they do not have independent information security event handling competency – except those organizations which the central infrastructure operator provides only a part of the service for (e.g. infrastructure (IaaS) or platform (PaaS). At the same time, these organizations have to protect their information systems which they can use as a service from a provider with adequate competency, who can be a market participant, but in case of administrative bodies, the central infrastructure provider.

Independently from the type of the provider, the functions, the responsibility, the limits, and the technical conditions for providing service have to be defined in detail.

If the laws allow it, security operation can be imagined in several types of operation models:

- The whole event and incident handling is done by the service provider in possession of a certain authorization, either by directly controlling the IT operational divisions or by configuring other service provider-operated system components.
- The service provider only alerts the organization to the security event, the whole investigation and responding is done by the organization with the help of data sent by the service provider or stored in its own systems.
- Differed in contract, any transitional solutions can be imagined between the two models, depending on the quality and quantity of resources the organization has. In case of cloud computing “Defined Categories of Service 2011” published by the Security as a Service Working Group of Cloud Security Alliance helps¹⁷.

¹⁷ Kovács Zoltán: *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai* Doktori Értekezés http://uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/kovacs_zoltan_2015.pdf (downloaded: 2017.06.01)

In case of a significant security event the organization can evolve in an ad hoc way or by law an external incident investigating organization (in case of public administrative bodies the GovCERT, in case of business organizations the service provider whose activity field is incident handling).

The incident handler operating in either model may have access to legally protected data (mostly personal, sensitive data and business secrets). In case of business secrets, data handling and accessibility can be regulated freely in a contract. In case of personal and sensitive data handling Act No. CXII. of 2011 on the right of informational self-determination and on the freedom of information (hereinafter: Privacy Act)¹⁸ imposes strict rules, including that all the conditions of personal data handling have to be regulated in a contract with the responsibility, functions and informing obligation of the parties.

If an organization outsources the security operation function, then the organization is advised to act in accordance with the recommendation published by the Hungarian National Authority for Data Protection and Freedom of Information in 2013.

The law in effect imposes rules on the central IT and electronic service provider appointed by law how to operate its systems securely, though does not give additional authorization for the service provider and does not define what the service provider can do and what data it can handle in interest of this. As long as the service provider provides security services, in the current legal environment it has to agree on the terms of data processing/data handling with all the parties and regulate it in contracts. Regarding the circle and number of organizations concerned and the interest of protecting the handled data, it would be expedient to regulate the issue of data handling by laws, creating the bases of unified data handling during incident handling.

In interest of the requirements defined in Ibtv. and in the Privacy Act, it would be important to draw up recommendations for the professionals on – among others, in interest of the mass protection of personal data – what data the incident handler can handle, with what conditions the incident handler can look into that letter or netflow, with the help of which data leakage may be occurring, or other security event happens that concerns data handling or processing.

Summary

¹⁸ Act No. CXII. of 2011 on the right of informational self-determination and on the freedom of information https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (downloaded: 2017.06.01)

To protect information systems effectively – beside the traditional solutions – it should be ensured that logs of events in information systems are made, these logs are sent to the analyzing systems and the recognition and handling of security events occur. Beside the information generated during incident prevention and handling, indicators of harmful activity coming from external sources are very important. In many cases, the inclusion of co-areas is needed as well as in the practical realization of responding to incidents.

Above the technological and processual conditions there is a special importance to legal adequacy, mostly to Privacy Act, because the incident handler has to handle personal data (IP addresses, e-mail addresses, login names etc) inevitably during an incident. Even though the practice has been changing lately, it could not be said that it is uniform and – as far as I know – it has not been audited yet by the data protection authority.

References

- Act No. Act L. of 2013. on the electronic information security of the government and local governments
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (downloaded: 2017.06.04)
- Act No. CLXVI. of 2012. on the identification, designation and protection of critical infrastructures and facilities
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (downloaded: 2017.06.04)
- Act No. CXII. of 2011 on the right of informational self-determination and on the freedom of information
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (downloaded: 2017.06.01)
- Joseph MUNIZ, Gary MCINTYRE, Nadhem ALFARDAN: Building, Operating, and Maintaining Your SOC CISCO Press 2016 ISBN-13: 978-0-13-405201-4
- Kovács Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai Doktori Értekezés
http://uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/kovacs_zoltan_2015.pdf (downloaded: 2017.06.01)
- MITRE Carson Zimmerman: Ten Strategies of a World-Class Cybersecurity Operations Center
<https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf> (downloaded: 2017.06.04)
- MUHA Lajos: Útmutató az informatikai biztonság megvalósítására önkormányzatok számára
http://www.kormanyhivatal.hu/download/0/1a/00000/it_biztonsag_onkormanyzatoknak.doc (downloaded: 2017.06.01)
- NIST 800-61 Computer Security Incident Handling Guide Special Publication Revision 2
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (downloaded: 2017.06.04)
- Oliver Rochford, Paul E. Proctor: Innovation Tech Insight for Security Operations, Analytics and Reporting
<https://www.gartner.com/doc/3166239/innovation-tech-insight-security-operations> (downloaded: 2017.06.02)
- Regulation of the Government No. 185/2015. (VII. 13.) on the governmental incident handling center and its functions and authority, and on the rules of security incident handling, the security incident's

technical investigation and on the carrying out of the vulnerability testing process

https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
(downloaded: 2017.06.04)

- Regulation of the Ministry of Interior No. 41/2015 (VII. 15.) on the technological security, the secure informational devices, products and the requirements of classification to security category and security level defined in Act No. L. of 2013 on the electronic information security of the government and local governments
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV
(downloaded: 2017.06.04)
- SÁGI Gábor: Informatikai rendszerek naplózása (Nemzetbiztonsági Szemle MMXVII/I)
http://uni-nke.hu/uploads/media_items/sagi-gabor-az-informatikai-rendszerek-naplozasa.original.pdf (downloaded: 2017.06.04)

A nemzetbiztonsági stratégiáról a Nemzeti Katonai Stratégia tükrében

Drusza Tamás¹

Absztrakt:

Alábbi tanulmányában a szerző áttekinti a katonai és a nemzetbiztonsági terület kapcsolódási pontjait, az ágazati stratégiák szükségességének kérdését, a stratégiák szerepét. Elemzi a nemzetbiztonsági ágazati stratégia késlekedésének okait, lehetséges magyarázatait, összehasonlítva ezeket a Nemzeti Katonai Stratégia megszületésének körülményeivel. Röviden bemutatja az USA hírszerző közösségében végbement stratégiai fejlődés eredményeit, végül röviden megvizsgálja a nemzetbiztonsági stratégia jövőben kilátásait.

Kulcsszavak: stratégia, nemzetbiztonság, jövő, hatékonyság

Abstract:

In the following study the author gives a comprehensive review of national security - military interfaces, and the question of the necessity and role of sector strategies. The author analyzes causes and possible explanations of delay in strategy of national security, comparing them with the circumstances of the National Military Strategy formation. Briefly presents the strategic development outcomes of the US intelligence community, finally provides a short evaluation of the future prospects of forming strategy in the field of national security.

Keywords: strategy, national security, future, efficiency

¹ drusza.tamas@uni-nke.hu, ORCID azonosító: [orcid.org: 0000-0003-2274-6789](https://orcid.org/0000-0003-2274-6789)

Bevezetés

A nemzetbiztonsági közgondolkodásban régóta visszatérő téma a hiányzó nemzetbiztonsági stratégia témaköre. A stratégiai tervek kidolgozása és végrehajtása, mint eszköz, a katonai tevékenységhez kötődően alakult ki, ahol a létért folytatott küzdelemben² számos erőforrást kell optimális módon kombinálni a kitűzött célok érdekében. Veszprémy László megfogalmazásában a stratégia „... *tágabban értelmezve a fegyveres erőknél a katonai célok elérésének érdekében való alkalmazása, s még további kiterjesztéssel, magának a háborús politikai célnak a megvalósítása.*”³ Megítélésem szerint nem kell részletesen indokolni, hogy egy hadsereg felállítása, felkészítése és alkalmazása milyen nagy léptékű, összetett és hosszú távú gondolkodást igénylő feladat. Azóta a stratégiai menedzsment a vezetés- és szervezéstudomány hangsúlyos részterületévé vált, átültetve e szemléletet a polgári életbe, és lényegesen tovább is fejlesztve azt.⁴

Társadalmi funkcióját tekintve a nemzetbiztonsági terület sok tekintetben hasonlóságot mutat a katonai területtel. Mindkettő a társadalmi biztonságért felelős, összetett, nagy erőforrásokat felhasználó rendszer. Mindkettőnek elsődleges feladatai között szerepel az ország védelme, függetlenségének, szuverenitásának biztosítása, ellenérdekelte külső hatalmak és szervezetek támadásainak felderítése, kivédése, amelyekhez a hagyományos államigazgatási rendszertől eltérő speciális eszközök és módszerek, illetve felhatalmazás áll rendelkezésükre. Végül, de nem utolsó sorban, mindkét terület kudarca - akár egyetlen nem kívánatos esemény bekövetkezése esetén is - súlyos veszteség és hátrány érheti az adott országot, társadalmat. Ezen körülmények nem csak hatalmas felelősséget tesznek az érintett terület szervezeteinek és szakembereinek vállára, hanem alapjaiban indokoltá teszik a hadászati, azaz stratégiai megközelítés, tervezés alkalmazását mindkét tevékenység esetében. Magyarország Nemzeti Katonai Stratégiája, bár jelentős csúszással, de 2009-ben, immár nyolc éve elkészült, 2012-ben frissítésre is került. A nemzetbiztonsági ágazati stratégia, azóta is várta magára.

Nemzetbiztonsági stratégiára várva

„A Magyarország biztonságát és védelmét veszélyeztető fenyegetések kivédésére megfelelően felkészülni, a megelőző vagy válaszlépések (akadályozás, korlátozás,

² TÁLAS Péter: *A nemzeti katonai stratégia és a magyar stratégiai kultúra*, in. *Hadtudomány 2013/3-4.* 16. o.

³ VESZPRÉMY László: *A modern hadtudomány megszületése*, in. VESZPRÉMY László (szerk.): *A korai stratégiai gondolkodás.* Zrínyi Kiadó, 2005, 7. o.

⁴ MINTZBERG, Henry – AHLSTRAND, Bruce – LAMPEL, Joseph: *Stratégiai Szafari.* HVG Kiadó, 2005, 29. o

„bomlasztás” és megszakítás) megtételére csak komplex, hosszabb időtávra érvényes titkosszolgálati stratégia birtokában van lehetőség”⁵ Ezt a gondolatot Lénárt Ferenc fogalmazta meg, 2001-ben, több mint 16 évvel ezelőtt. Ekkor még nem, illetve csak körvonalaiiban⁶ létezett az a Magyarországra vonatkozó átfogó biztonsági stratégiai dokumentum, amelynek - figyelembe véve a stratégiai hierarchiát - egyfajta keretet és alapot kell(ene) nyújtania a nemzetbiztonsági stratégia elkészítéséhez. Lénárt maga is kifejti, hogy egy ilyen stratégia megalkotását megelőzően szükséges vizsgálni Magyarország szélesebb értelemben vett biztonsági helyzetét.⁷ Erre ma a Nemzeti Biztonsági Stratégia (NBS) hivatott.

Mikor 2012-ben megjelent Magyarország harmadik Nemzeti Biztonsági Stratégiája,⁸ újból felmerült a remény a nemzetbiztonsági stratégia belátható időn belüli megjelenésére. A Nemzeti Biztonsági Stratégia ugyanis, számos hiányosságra ellenére megteremtette az alapokat, amelyekre építkezve ki lehetett volna dolgozni a nemzetbiztonsági ágazat közép- és hosszú távú működési koncepcióját. Már a 2004-es NBS is tartalmazott származtatott területek, így a nemzetbiztonsági terület stratégiájának kialakítására vonatkozó megállapítást és kötelezettséget, és a 2012-es változat is tovább vitte ezt a gondolatot.⁹ Mindezek ellenére - jóllehet a téma szakirodalma számos ezzel foglalkozó írással gazdagodott¹⁰ - a nemzetbiztonsági stratégia azonban mai napig nem látott napvilágot. Véleményem szerint érdemes megvizsgálni, milyen körülmények és okok vezethettek ide.

A körülmények áldozata?

A szakirodalomban, általánosságban véve szinte egységes az a szakértői álláspont, hogy nemzetbiztonsági stratégiára szükség van. Emellett a szakma művelői számára is fontos iránymutatást jelentene, illetve a kormányzat is tett ez irányba lépéseket¹¹ mégsem sikerült elkészíteni és elfogadni egy ilyen jellegű átfogó dokumentumot. Feltételezhető, hogy ez számos olyan körülmény közös eredményére vezethető vissza, amelyek együttesen hatva komolyan hátráltatják e - stílszerűen szólva - stratégia fontosságú dokumentum megszületését. A stratégia gon-

⁵ LÉNÁRT Ferenc: *Biztonság, nemzetbiztonság. Új Honvédségi Szemle, 2001/1., 52. o.*

⁶ Magyar Köztársaság biztonság- és védelempolitikai alapelveiről szóló 94/1998. (XII.29.) Országgyűlési határozat.

⁷ LÉNÁRT Ferenc: *uo. 52-53. o.*

⁸ Eddig háromszor került sor Nemzeti Biztonsági Stratégia kiadására: 2002, 2004, 2012

⁹ SOLTI István: *A nemzetbiztonsági stratégia a Nemzeti Biztonsági Stratégia tükrében, Nemzetbiztonsági szemle 2014/3 48-49 o. alapján*

¹⁰ DÁVID Ferenc: *Az új évezred nemzetbiztonsági feladatellátásának súlypontjai, Nemzetbiztonsági szemle 2015/1., 201. o.*

¹¹ SOLTI István: *uo. 49-50 o.*

dolgozás lépcsőfokain haladva adódik a megállapítás, hogy ezen okok megszüntetéséhez vezető út első lépése az okok számbavétele kell, hogy legyen.

1. Stratégia nélkül is működőképes a szervezetrendszer

Kétségtelen tény, hogy számos szervezet működik stratégiai terv nélkül. Sőt a stratégiai menedzsment szakirodalom sem gondolja mindenhatónak a formális stratégiákat. A terület egyik legnagyobb hatású szaktekintélye Henry Mintzberg és munkatársai 2005-ös könyvükben (Stratégia Szafari) számos olyan stratégiaalkotási irányzatot bemutatnak, amelynek nem része a formális tervezés.¹² Abban azonban szerintük is egyetértés van, hogy még a kevésbé vagy egyáltalán nem formalizált stratégiák is többek között

- a változó környezet kezelésére hivatottak;
- a nem rutinszerű dolgokról szólnak;
- hatással vannak a szervezetek általános boldogulására;
- érintik a tartalom és a folyamat kérdéseit is;
- összességében a lényeges dolgok kezelésére hivatottak.¹³

Mintzbergék szerint a stratégiák legfontosabb jellemzője, hogy *„megoldja a nagyobb ügyeket s így az emberek már elboldogulhatnak az apróbb részletekkel...”*¹⁴

Az általuk felvázolt egyes iskolák megközelítésmódjai különböző körülményeket feltételeznek. Ebből a szempontból a nemzetbiztonsági terület és szervezetrendszer azok közé tartozik, amelyek kifejezetten igényelhetik a megtervezett, formalizált stratégiákat, mert:

- a szervezetek funkciója adotttság;
- a környezeti változások nagy bizonyossággal előre jelezhetők;
- a szervezetek erősen formalizáltak, irányíthatóak;
- a felelősségi és hierarchikus viszonyok egyértelműek;
- a szervezetek tevékenysége között erős átfedések mutatkoznak.

A szakirodalomban is számos szerző számtalan érvet felsorakoztatott már a nemzetbiztonsági stratégia mellett, emellett azonban arra a kétségbevonhatatlan tényre is rámutattak már, hogy a nemzetbiztonsági szolgálatok leírt stratégia nélkül is működőképesek maradtak.¹⁵

Csiki Tamás általánosságban így fogalmazta meg a biztonsági stratégiai funkcióját: *„Reális biztonságpolitikai célokat meghatározni és ezekhez eszközöket*

¹² MINTZBERG, Henry – AHLSTRAND, Bruce – LAMPEL, Joseph: *Stratégiai Szafari*. HVG Kiadó, 2005

¹³ MINTZBERG-AHLSTRAND-LAMPEL: uo. 27. o

¹⁴ MINTZBERG-AHLSTRAND-LAMPEL: uo. 28. o

¹⁵ DÁVID: uo. 203. o.

rendelni – azaz stratégiát alkotni –, majd mindezt megvalósítani a nemzetközi környezet bármely változása mellett: ez minden racionálisan gondolkozó, hosszú-távra tervező állam alapvető érdeke. Ezáltal biztosítható a nemzeti értékeken alapuló érdekek képviselése, a biztonságpolitikai kihívásokra választ adni képes, megfelelő katonai és civil – kemény és puha hatalmi – képességek kialakítása, a fejlődési célok hatékony megvalósítása.”¹⁶

2014-es írásában Solti István felteszi a kérdést, hogy ha ilyen hosszú ideig nem készült el a nemzetbiztonsági stratégia, akkor ez vajon azért lehet-e, mert e nélkül is remekül működik a terület és ebből következően nincs is rá szükség?¹⁷ Solti a saját maga által feltett kérdést akképpen válaszolja meg, hogy a stratégiára szükség van, hogy „... a politikai csatározások okozta gyakori struktúra változások és az elsődleges kormányzati elvárások egyértelmű kinyilvánításának hiányában megjelenő szektoron belül érzékelhető ágazati elbizonytalanodások ki-küszöbölhetőek legyenek”¹⁸.

Izsa Jenő 2007-es tanulmányában más érvek mellett az alábbi főbb indokokat hozza fel a nemzetbiztonsági stratégia szükségességének alátámasztására;¹⁹

- csak az ágazati stratégiák koherens rendszere biztosítja az optimális erőforrás elosztást;
- a benne foglaltak elvi útmutatót adhatnak a különböző nemzetbiztonsági szolgálatok feladatainak végrehajtásához és a szakmai tevékenységben szükséges korrekciók elvégzéséhez, úgy szabályozók megalkotásához;
- segíthet megteremteni az összhangot a nemzetbiztonsági szolgálatok és más nem ebbe a körbe tartozó, de titkosszolgálati eszközöket és módszereket alkalmazó szervezetek között;
- hosszú távú kiszámíthatóságot teremtené a hektikus belpolitikai viszonyok között.

A stratégia nélküli működőképesség vizsgálata valójában nem a probléma lényegét érinti. A stratégiák funkciója nem a szervezetek működtetése, így a kérdés nem az, hogy nemzetbiztonsági stratégia nélkül is működőképes marad-e az intézményrendszer. A probléma lényegét a hadászat és a harcászat analógiájával tudjuk a leginkább megvilágítani. Egy hadsereg harcászatiilag akkor is működőképes, ha nem rendelkezik megfelelő hadászati szintű tervekkel, ugyanakkor a megvívott csaták és meghozott áldozatok révén kifejtett erőfeszítés vélhetően nem segíti elő a hadsereg és az ország céljainak, érdekeinek érvényesülését.

¹⁶ CSIKI Tamás: *A magyar stratégiai kultúra vizsgálatának eredményei, biztonságpolitika.hu*, 2013.01.13.

¹⁷ SOLTÍ: uo. 48. o.

¹⁸ SOLTÍ: uo. 48. o.

¹⁹ IZSA Jenő: *Javaslatok a nemzetbiztonsági / titkosszolgálati stratégia kidolgozásához. Hadtudomány 2007/1. alapján*

A munkatársak hazaszeretete, elhivatottsága, rutinja, illetve a jogszabályok és a szakmai protokollok valóban képesek folyamatosan fenntartani a működőképességet, stratégia nélkül is. Ezen erőfeszítések hatékonyságát azonban jelentősen befolyásolják a közigazgatásra jellemző bürokratikus akadályok, koordinációs problémák, az erőforrások pazarlásával járó költséghatékonysági problémák, illetve a különböző nemzetbiztonsági szervezetek szétartó céljai. A stratégia, mint eszköz, ezen problémákra jelenthet megoldást, biztosítja a kitűzött célok elérését optimális erőforrás-felhasználás mellett.

2. A nemzetbiztonsági szféra szétagoltsága:

Jóllehet már a '80-as évek második felében munkacsoport dolgozott az állambiztonsági szervezetrendszer átalakításának lehetőségeivel,²⁰ a politikai döntéshozók végül a leginkább kézen fekvő és legegyszerűbb megoldást választották²¹: a Belügyminisztérium III. Főcsoportfőnöksége alatt működő csoportfőnökségeket önálló szolgálatokként szervezték újra, illetve megszüntették (III/III). Ennek keretében a rendszerváltáskor két polgári és két katonai szolgálattal állt fel az új nemzetbiztonsági struktúra.

E struktúra nem bizonyult időtállóknak. Már 1996-ban megtörtént az első változás: a Nemzetbiztonsági Hivatal szervezetéből leválasztották a technikai támogató feladatköröket és ezeket az újonnan létrejövő Nemzetbiztonsági Szakszolgálathoz delegálták. Az ezt követő bő évtizedben - különböző okokból - több koncepció készült²² egy modernebb és hatékonyabb struktúra kialakítása érdekében, de az érdemi változtatásokra 2010-ig kellett várni. Ekkor azonban a várt egyszerűsítés helyett a nemzetbiztonsági szervezetrendszer összetettebbé válása valósult meg. Kettőről háromra emelkedett az irányító minisztériumok száma, illetve a nemzetbiztonsági feladatok lényeges elemét (terrorelhárítás) egy más típusú feladatokat is ellátó rendőri szervezet (Terrorelhárítási Központ) vette át. 2012-ben a katonai szolgálatok összevonásából egy egységes hírszerző-elhárító szervezet jött létre (Katonai Nemzetbiztonsági Szolgálat). A szervezetrendszer mai formáját 2016-ban nyerte el a Terrorelhárítási Információs és Bűnügyi Elemző Központ megalakításával.

A három minisztérium irányításával, 5+1 nemzetbiztonsági feladatkörrel működő szolgálatra tagozódó struktúra kétségtelenül nem egyszerűsíti a nemzetbiztonsági stratégia kialakítására irányuló erőfeszítéseket. Már maga ez a struktúra is a különböző vélemények és a (látszólag) eltérő szervezeti érdekek mentén alakulhatott ki, ezek szövevényében nem könnyű megtalálni azokat a pontokat,

²⁰ KOVÁCS Zoltán András – DOBÁK Imre: *Korszakváltások a magyar nemzetbiztonsági intézményrendszerben*, in. SABJANICS- FINSZTER (szerk.): *Biztonsági Kihívások a 21. században*, Dialóg Campus, Budapest, 2017, 176-177. o

²¹ KOVÁCS – DOBÁK: *uo.* 178. o

²² KOVÁCS – DOBÁK: *uo.* 183-188 o.

amelyek segítségével közös nevezőre hozható a különböző szervezetek egymást sokszor átfedő tevékenysége. Ugyanakkor önmagában nem is lehetetlen, amelyet számos körülmény is alátámaszt.

1. Nemzetközi példaként, az Egyesült Államok Hírszerző Közössége említendő, amelynek 17 tagja van. Két független, közvetlen elnöki alárendeltségben működő szervezet, nyolc védelmi minisztériumhoz tartozó szervezet, és hét további olyan szervezet, amelyek öt egyéb minisztériumhoz tartoznak. E hírszerző közösség mégis rendelkezik egységes Nemzeti Hírszerzési Stratégiával (National Intelligence Strategy)²³. A széttagoltság problémáját az Egyesült Államokban úgy oldották meg, hogy létrehoztak egy koordinációs pozíciót (Direktor of National Intelligence) a hozzá tartozó apparátussal, amelynek feladata Hírszerző Közösség működésének stratégiai és operatív összehangolása.
2. A Nemzeti Biztonsági Stratégia elkészülte önmagában igazolja, hogy nem lehetetlen számos terület összhangjának megteremtése. Az NBS-ben lefektetett elvek is azt rögzítik, hogy szinte minden kormányzati szervnek, egymás munkáját kiegészítve, támogatva kell közreműködniük az ország biztonságának garantálásában.
3. *„2011-ben a kormány – a BM kezdeményezésére – újjászervezte a Nemzetbiztonsági Kabinet működését, amelynek üléseit ismét a miniszterelnök vezeti. A belügyi és a honvédelmi tárca vezetője közösen fogja össze a kabinetnek szakmai háttértámogatást nyújtó, döntéseket előkészítő Nemzetbiztonsági Munkacsoport működését, amelynek ülésein a nemzetbiztonsági szolgálatok vezetői mellett jelen vannak a rendvédelmi szervek országos parancsnokai is.”*²⁴ A Nemzetbiztonsági Kabinet és a Nemzetbiztonsági Munkacsoport nyújtotta keretek teljes mértékben alkalmasak lennének a nemzetbiztonsági stratégia kialakítására.

Paradox módon a nemzetbiztonsági szervezetrendszer tagoltsága nem csak nehezíti a nemzetbiztonsági ágazati stratégia létrejöttét, ugyanakkor fokozottabb mértékben igényelné is. Ebben az esetben a stratégia ugyanis egyfajta koordinációs mechanizmus szerepét is betöltené, a célok és erőforrások összerendelése révén. A 2001-es terrortámadásokat követően vélhetően e felismerés is közrejátszott abban, hogy az USA-ban önálló koordinációs intézményt²⁵ alakítottak ki a titkosszolgálati tevékenység összehangolására. A hírszerzési stratégia kidolgozása és végrehajtása e koordinációs feladat egyik legfontosabb része.

²³ <https://www.dni.gov/index.php/what-we-do/members-of-the-ic> (letöltve: 2017.09.05.)

²⁴ KOVÁCS – DOBÁK: uo. 191. o.

²⁵ Director of National Intelligence (Nemzeti Hírszerzési Igazgató)

3. A magyar stratégiai kultúra színvonala

A magyar tudományos életben a stratégiai kultúra vizsgálata egészen újszerű témának számít. A témában eddig született néhány tanulmány mindegyike biztonságpolitikai, sőt első sorban katonai szempontból vizsgálja a kérdést. Témánk szempontjából Tóth Péter 2013-as tanulmánya a leginkább releváns, amely többek között arra keresi a választ, hogy a miért csak a NATO csatlakozás után 10 évvel, az első NBS után 7 évvel, 2009 készült el az első Nemzeti Katonai Stratégia (NKS), amit aztán rögtön három évvel később felül is kellett vizsgálni. Véleménye szerint az okok között *„vannak objektív és szubjektív okok, általános európai jelenségek, kelet-közép-európai regionális jellemzők és speciálisan magyar sajátosságok egyaránt.”*²⁶

Az európai jellemzők között első sorban azt említi meg, hogy például az USA-hoz viszonyítva, Európában még mindig a „fehér-könyv” jellegű „stratégiák” dominálnak, nem pedig a célok és erőforrások összhangját megteremtő tervek. A „fehér-könyv” kifejezést azokra a dokumentumokra szokták használni, amelyek egy adott szervezet bizonyos témáról alkotott véleményét, elvárásait, céljait fekteti le. Példának okáért a német, de a magyar NBS is ezt a koncepciót követi.

A közép-európai országok problematikájának számbavételkor Tóth két fő okot vázol fel. Első helyen azt említi meg, hogy ezekben az országokban a rendszerváltás után a hadsereg kérdésköre általánosságban nem élvezett kiemelt prioritást. Az ezen országok által örökölt szovjet mintájú, túlméretezett, diszfunkcionálissá váló hadsereg és a 21. századi kihívások, elvárások között olyan ellentmondás feszült, amelynek feloldása a rendszerváltás körüli forráshiányos helyzetben politikailag nem volt vállalható. Második helyen azt vázolja, hogy ezen országoknak egyszerre kellett megküzdeniük a nemzettudat újjáépítésének (renacionalizáció), az európai integrációba való bekapcsolódás és a globalizációhoz való alkalmazkodás sokszor egymásnak ellentmondó nehézségeivel.²⁷ Ez az ellentmondásos helyzet nem tette lehetővé egyértelmű és konszenzusos célok kijelölését.

Magyarország tekintetében - számos más szerzőhöz hasonlóan - a politikai konszenzus hiányában, mint fő tényezőben látja a stratégiaalkotásban tapasztalt lemaradást. A társadalmilag fontos kérdésekben alkotott konszenzus egyértelmű feltétele annak, hogy hosszabb távra alkotott stratégiák eredményesen végrehajthatóak legyenek. Lengyel minta alapján megemlíti továbbá annak szükségességét, hogy a megválasztott politikusok alapvető biztonságpolitikai, illetve modern stratégiai ismertekhez és szemlélethez jussanak, mielőtt elfoglalják hivatalukat.²⁸

²⁶ TÓTH: uo. 17. o.

²⁷ TÓTH: uo. 22-23.o

²⁸ TÓTH: uo. 22. o.

Témánk szempontjából a legfontosabb kérdés, hogy a katonai stratégiával kapcsolatos fenti megállapítások párhuzamba állíthatók-e a nemzetbiztonsági stratégia elmaradásával. Hasonló okok magyarázhatják-e ennek lassan évtizedekben mérhető késését, vagy más körülmények játszanak közre. Ahogy azt már leszögeztük: a nemzetbiztonsági terület a védelmi területhez hasonlóan a biztonság szavatolásának az ország érdekérvényesítésének eszköze és így az általános geo-, biztonságpolitika kérdéskörtől el nem választható. Szintén nehezen vitatható, hogy mind a rendszerváltás előtti állambiztonsági rendszer nehéz öröksége, mind a társadalmi átalakulás kihívásai hasonlóan nehezítették a hosszú távú koncepciók kialakítását. Végül, bár eleinte látszott remény az ellenkezőjére, nemzetbiztonsági területen sem alakult ki az a szükséges társadalmi konszenzus, amely szilárd alapokon álló hosszú távú célrendszer alapját jelenthette volna. Szintén nehezen vitatható, hogy az ágazati stratégia szempontjából a szükség és sürgősség érzetének kialakulását az sem segítette elő, hogy az államigazgatás egészére jellemző a stratégiai szemlélet hiánya, illetve a stratégiákban való gondolkodás alacsony színvonala.

A két ágazat közötti jelentős különbség, hogy a nemzetbiztonsági szervezetrendszer tagoltabb, de méretei sokkal kisebbek, így az esetleges változtatások kisebb társadalmi költséggel végrehajthatóak lennének. Ezt az is mutatja, hogy már közvetlenül a rendszerváltás után egy új rendszer állt fel, amit azóta számtalanszor módosítottak is. Ebből következően feltételezhető, hogy nem elsősorban a szervezetrendszer átalakításának társadalmi költségei vagy hasznai játszottak és játszanak döntő szerepet a stratégia késlekedésében. Vannak azonban más hatások, amelyek kifejezetten a nemzetbiztonsági területhez köthetőek és számottevően akadályozhatták a stratégia megszületését. Ebből a szempontból még mindig kísért a múlt: a politika és ettől vélhetően nem függetlenül a szakma is ódzkodik a nemzetbiztonsági relevanciájú kérdések nyilvános, társadalmi szintű megvitatásától. A rendszerváltás előtt, amikor is az állambiztonság részt vett a társadalom elnyomásában, ez egy „természetes” helyzet volt. Jogállamban azonban ez a fajta nyilvános vita nem kerülhető meg, és a nemzetbiztonsági intézményrendszer számára létfontosságú társadalmi bizalom szempontjából nézve ez nem is célszerű.

Egy külföldi példa

Kétségtelen, hogy az Egyesült Államok nem csak a privát szférában, de az államigazgatás egyéb területein, így a biztonsági tevékenység esetében is élen jár a stratégiai menedzsment alkalmazásában. A 2001-es terrortámadások után pár évvel létrehozott stratégiai koordinációs intézmény elmúlt 13 éves működése²⁹ iskolapéldája annak, hogy a célok és erőforrások stratégia alkalmazásával megte-

²⁹ <https://www.dni.gov/index.php/who-we-are/history> alapján (letöltve: 2017.09.05.)

remtett összhangja, miként képes fokozni egy olyan rendszer eredményességét, amely azt megelőzően is világviszonylatban egyedülálló erőforrások és képességek birtokában volt. Miután 2004 decemberében a 9/11 Kongresszusi Bizottság közzétette a jelentését, az Intelligence Reform and Terrorism Prevention Act hatályba lépésével megkezdődött a Hírszerző Közösség³⁰ (Intelligence Community) radikális átalakítása. Ennek egyik legfontosabb lépése a Nemzeti Hírszerzési Igazgatói (Director of National Intelligence /DNI/) poszt és a hozzá kapcsolódó apparátus létrehozása volt (Office of the Director of National Intelligence /ODNI/). A szervezet fő feladata a titkosszolgálati információgyűjtő tevékenység, az ezért felelős szervezetek stratégiai irányítása és koordinációja lett.

Ennek elősegítése érdekében 2005-ben elkészítették az Egyesült Államok első Nemzeti Hírszerzési Stratégiáját.³¹ E stratégia mottója jól tükrözte az azt követő évtizedekben követett célt: „Transformation through Integration and Innovation”. Ezt követően a stratégia 2009-ben és 2014-ben felülvizsgálatra került. Figyelmet érdemlő, hogy a DNI működése óta eltelt 12 évben:

- Az Egyesült Államok területén nem történt eredményes külföldi szervezet által végrehajtott, tömeges áldozatot követelő merénylet, jóllehet az USA vezető szerepet vállalt a terror ellenes fellépésben. Ezzel szemben például Európában számos, sok áldozatot követelő merényletre került sor.
- Felderítésre és likvidálásra került Osama Bin Laden és számos más régóta keresett terrorista vezető.
- Az USA világszerte offenzíven, saját területükön tud fellépni a terrorszervezetekkel szemben.

Természetesen nem állíthatjuk, hogy mindez kizárólagosan a DNI által kidolgozott és végrehajtott NIS-nek köszönhető, de az megállapítható, hogy az Egyesült Államok hírszerző közössége terrorellenes erőfeszítéseinek eredményessége látványos fejlődésen ment keresztül az elmúlt bő évtizedben.

Mit hozhat a jövő?

Mivel a Nemzeti Biztonsági Stratégia felülvizsgálata jelenleg folyamatban van³², annak elfogadásáig nem várható a nemzetbiztonsági ágazati stratégia kidolgozá-

³⁰ Az amerikai terminológia szerint a hírszerzés, nem kizárólag azokat a szervezeteket jelöli, amelyek külföldi irányultsággal gyűjtenek információkat, hanem minden olyan titkosszolgálati eszközöket és módszereket használó szervezeteket, amelyek az Egyesült Államok biztonságaért felelősek.

³¹ <https://www.dni.gov/files/documents/CHCO/nis.pdf> (letöltve 2017.09.12.)

³² Magyar Közlöny, Hivatalos értesítő 58/2016. 45-46. o
<http://www.magyarokozlony.hu/dokumentumok/3f3c9e9fd2262037dbfb71baa461b01ef33323f/megtekintes> (letöltve: 2017.09.12.)

sának megkezdése. A fentiek alapján rövid- és középtávon alacsony a realitása az átfogó nemzetbiztonsági ágazati stratégia megszületésének.

Ugyanakkor nem mondhatjuk, hogy ez azt jelenti, hogy a nemzetbiztonsági területen nem jelenhetnek meg stratégiai gondolkodás olyan kis csírai, amelyek egyrészt hozzájárulhatnak a későbbi ágazati stratégia megszületéséhez, másrészt – például szervezeti stratégiák, funkcionális (pl. humánpolitikai) stratégiák formájában támogatnák a hatékonyabb működést, a stratégiai kultúra fejlődését. Ez annál is kívánatosabb volna, mivel újabb jelentős társadalmi változások (Z és alpha generációk, ipari forradalom 4.0³³) küszöbén állunk és kívánatos lenne, ha a nemzetbiztonsági szféra élen járna a változásokra felkészülés tekintetében, példát mutatva ezzel más területek számára is.

A nemzetbiztonsági terület stratégiai terv mentén történő működésnek lehetne még egy - általában kevésbé említett - pozitív mellékhatása is: fejleszthetné a területen tevékenykedő szakemberek általános stratégiai szemléletmódját, elősegítve ezzel a működés hatékonyságának javítását alacsonyabb (pl. alágazati, szervezeti) szinteken is. Egy modern nemzetbiztonsági stratégia azonban mindekelőtt egyértelmű üzenet lenne a magyar társadalom számára. A politika és a szakma is túllépett a terhes múlton, komolyan veszi a nemzet biztonságát és tudatosan igyekszik e területet fejleszteni, a 21. század követelményeihez igazítani.

Felhasznált irodalom:

- CSIKI Tamás: A magyar stratégiai kultúra vizsgálatának eredményei, biztonságpolitika.hu, (2013.01.13.)
- DÁVID Ferenc: Az új évezred nemzetbiztonsági feladatellátásának súlypontjai, Nemzetbiztonsági szemle 2015/1.
- IZSA Jenő: Javaslatok a nemzetbiztonsági / titkosszolgálati stratégia kidolgozásához. Hadtudomány 2007/1.
- KOVÁCS Zoltán András – DOBÁK Imre: Korszakváltások a magyar nemzetbiztonsági intézményrendszerben. in. SABJANICS- FINSZTER (szerk.): Biztonsági Kihívások a 21. században, Dialóg Campus, Budapest, 2017,
- LÉNÁRT Ferenc: Biztonság, nemzetbiztonság. Új Honvédségi Szemle, 2001/1.
- MINTZBERG, Henry – AHLSTRAND, Bruce – LAMPEL, Joseph: Stratégiai Szafari. HVG Kiadó, 2005.
- SOLTÍ István: A nemzetbiztonsági stratégia a Nemzeti Biztonsági Stratégia tükrében. Nemzetbiztonsági szemle 2014/3.

³³http://www.portfolio.hu/vallalatok/it/a_ma_ismert_vilagot_totalisan_elsopri_a_negyedik_ipari_forradalom.10.237125-3.html (letöltve: 2017.09.12)

- TÁLAS Péter: A nemzeti katonai stratégia és a magyar stratégiai kultúra, in. Hadtudomány 2013/3-4.
- VESZPRÉMY László: A modern hadtudomány megszületése, in. VESZPRÉMY László (szerk.): A korai stratégiai gondolkodás. Zrínyi Kiadó, 2005.

Internetes források:

- <https://www.dni.gov/index.php/what-we-do/members-of-the-ic> (letöltve: 2017.09.05.)
- <https://www.dni.gov/index.php/who-we-are/history> alapján (letöltve: 2017.09.05.)
- Magyar Közlöny, Hivatalos értesítő 58/2016. 45-46. o <http://www.magyarkozlony.hu/dokumentumok/3f3c9e9fd2262037dbfb71baa461b01ef333323f/megtekintes> (letöltve: 2017.09.12.)
- http://www.portfolio.hu/vallalatok/it/a_ma_ismert_vilagot_totalisan_el_sopri_a_negyedik_ipari_forradalom.10.237125-3.html (letöltve: 2017.09.12)

A terrorizmus és indirekt hatása a kiberterében

Simon László¹ – Dr. Magyar Sándor²

Absztrakt

A szerzők általános rendszerszintű látásmóddal közelítik meg a terrorista cselekmények hatását kifejezetten Európa kiberterére, induktív módon európai esetekből kiindulva vonnak le általános következtetéseket. Az ISIS³ azzal fenyeget, hogy halálos kimenetelű kibertámadásokat tervez a jövőben. A terroristák új dimenzióban támadják az egyének biztonságát. Fegyveres harcuk során a gerillákhoz hasonlóan az információt helyezik műveleteik központjába. A média szerint a terroristák harcában az információ és a kommunikáció egyszerre lehet halálos és nem halálos fegyver is. A cikk összegzése szerint az internetet fenyegetésre használó arctalan bűnözők csak indirekt módon ölhetnek ki életeket.

Kulcsszavak: terrorizmus, kibertámadás, gerilla hadviselés, információs környezet, információ- és hálózat-centrikus hadviselés hadikultúrája

Abstract

The authors make a general approach and system-wide effect of terrorist attacks specifically on the cyberspace of EU. Inductively starting from European cases and makes an overall conclusion. According to ISIS' threat, 'fatal' cyber-attacks are planned for the future. The terrorists are attacking to the security of individuals in a new dimension. During their harmed struggle, they put the information on central of their operations like the guerrillas. The media said the information and the communication can be and not can be deadly weapon at a time in the terrorist war. According to a summary of the article faceless criminals use the internet to the threat, that these acts are killing only.

Keywords: terrorism, cyber-attack, guerrilla warfare, information environment, war culture of information- and network- centric warfare.

¹ NKE NBI, szakoktató, e-mail: simon.laszlo@uni-nke.hu

ORCID ID: 0000-0001-6771-8621

² NKE NBI, egyetemi adjunktus, e-mail: magyar.sandor@uni-nke.hu

Orcid ID: 0000-0002-6085-0598

³ ISIS: Az Iszlám Állam elnevezésű terrorszervezet (*Islamic State of Iraq and Syria*) angol rövidítése.

Bevezetés

A 20. század második felében a világ technikai környezete forradalmi változásokat élt meg. Az információ és a digitális tudás került a figyelem középpontjába, továbbá az innovatív ipari fejlesztések előterébe is. Az addig ismert és biztonsági szempontból is jól kontrollált környezetünk teljesen megváltozott. A társadalmi, politikai, gazdasági, szociális és nem utolsósorban katonai előnyöket is magába rejtő digitális technológia megvalósítása olyan információs és infokommunikációs hálózatok kialakítását jelentette, amelyek nem csak a technikai rendszerekre, de az emberi kapcsolatokra is hatást gyakorolhat.⁴ A posztmodern társadalmakban⁵ az emberek együttélésének új, határokat nem ismerő, idillikus (szabad, boldog és békés) képe született meg. Az életünket a globalizáció, illetve a személyes és elektronikus kapcsolatok bonyolult viszonyrendszere egyszerre azzal a reménnyel kecsegtette, hogy az információkhoz időben és igényeink szerint, akár korlátlanul is hozzáférhetünk. Ez a technológiai távlatokban is rövid forradalom a 21. századra kiépítette az információs társadalmakat.

A globalizáció és az információs hálózatok elterjedése katalizátorként hatott az 1991-ig fennálló bipoláris világ megszűnésére. Politikai, jogi és biztonsági szempontból a két világhatalom, az Amerikai Egyesült Államok (USA) és a Szovjetunió (SZU) – illetve a hozzájuk kapcsolódó katonai tömbök – viszonylag statikus, de mindenképpen kiszámíthatóbb környezetet jelentettek az országok élete, fejlődése szempontjából. A SZU felbomlása után nem sokkal szertefoszlott az idillikus jövő képe. A 2001. szeptember 11-i terrortámadást követő politikai és katonai lépések – a már említett hálózatokon megjeleníthető információkkal – új fenyegető és gyakorta arctalan ellenséget teremtettek. Az addig hagyományos és reguláris módon folytatott „kis háborúk”, illetve fegyveres küzdelmek⁶ kiléptek a földrajzi környezet által meghatározott fizikai térből. Az al-Kadía és az Iszlám Állam (ISIS) elnevezésű terrorszervezetek mára ezeken az említett földrajzi

⁴ SIMON László: *Az információ mint fegyver?* In: *Szakmai Szemle* 2016. 1. sz. pp. 34-60.

⁵ *Az amerikai gondolkodók a 19. század végén arra a felismerésre jutottak, hogy a politika nemcsak nemzetállami kereteken belül, hanem globálisan is értelmezendő. A társadalomelméleti következtetésekben kimondták, hogy az emberek életében politika nem lehet beavatkozó. A posztmodern (modern utáni) felfogásként illetett politikának szolgálóvá és segítővé kell válnia.* Európában Jean-François Lyotard a „La condition post-moderne” című 1979-es művében használta a fogalmat először, amikor a késői ipari (posztindusztriális) társadalom és a plurális demokrácia után megjelenő társadalomelméleti lehetőségeket elemezte. In: BOROS János: *Jean-François Lyotard, a különbözőség elgondolója, Kísérlet egy tudáselméleti megközelítésre. Jelenkor: Irodalmi és Művészeti Folyóirat*, XLII. évf. 3.sz. 1999. pp. 298-306.

⁶ RESPERGER István, KISS Álmos Péter, SOMKUTI Bálint: *Aszimmetrikus hadviselés a modern korban – Kis háborúk nagy hatással.* Zrínyi Kiadó, 2014. pp. 13-44.

területeken megerősödve, a lakosságot megnyerve vagy megfélemlítve, kvázi államként képesek fenntartani hatalmukat. Cikkünkben arra keressük a válaszokat, hogy a szervezetek által végrehajtott támadásokban és a hatalom megszerzése, fenntartása területén milyen szerepe lehet az információs hadviselésnek. Feltevésünk szerint az ellenük eddig alkalmazott hagyományos hadviselés módszerei mellett sokkal jobban kell koncentrálni az információs, illetve az infokommunikációs hálózatok nyújtotta lehetőségekre, mert a kibertér jelenleg a terrorizmus egyik legalkalmasabb eszköze a politikai és a katonai célok elérése érdekében.⁷

Az információs műveletek és környezetük jelentősége a kibertérben

Az információs forradalom egyik következményeként a klasszikusan elkülöníthető társadalmi, természeti és technikai környezetek egyre inkább átfedik egymást. A modern kori problémák megközelítése, illetve hatékony megoldása holisztikus elemzést és értékelést igényel.

Elgondolásunk szerint a tudományos elemzési modellek elsősorban egy adott tudományterület mélységi kutatásait erősítik. Egyes területek érintkezésekor szükséges vizsgálatok interdiszciplináris megközelítése miatt, akaratlanul is ellenmondás, illetve tudományos értelemben vett versenyhelyzet alakulhat ki. A tudomány a kutatási eredmények szigorú kritikája és a vitája során haladhat előre.⁸ A kibertér kutatására ez hatványozottan igaz. Minél inkább szeretnénk megismerni azt, annál kevésbé tudunk egy-egy tudományág önálló megállapításaira hagyatkozni. Véleményünk szerint a kibertér egyszerre lehet technikai és társadalmi rendszer, ugyanakkor a természeti struktúrákhoz, organizmusokhoz hasonló, akár természeti törvényszerűségeket mutató virtuális környezetként is felfogható.

Ezt a szemléletet követve az európai kiberteret a Haig Zsolt által választott hármas egységben közelítettük meg.⁹ Az információ, a társadalom és a biztonság összefüggéseiben folytatott kutatás alapját így nemcsak a fizikai eszközök (hardverek) működésére és kapcsolataira lehet alapozni, hanem a társadalomra és az életünket meghatározó mindennapi folyamatokra, illetve következményekre is. A terrorista csoportok tevékenységét és a terrort (agressziót) elsősorban ebben a térben folytatott, illetve közvetített folyamatok összehatásaként értelmeztük. A terrorszervezetek célja ideológiáktól és vallásoktól függetlenül közvetve vagy közvetlenül politikai háttérrel bírt. A célpontok tekintetében első

⁷ HAIG Zsolt: *Információ, Társadalom, Biztonság*. NKE Szolgáltató Kft, 2015. pp. 93-122.

⁸ BERÉNYI Dénes: *Hogy látja ma egy fizikus a világot?*

<http://vigilia.hu/regihonlap/2010/7/berenyi.html> (Letöltés ideje: 2017. 09. 15.)

⁹ HAIG Zsolt: *Információ, Társadalom, Biztonság*. NKE Szolgáltató Kft, 2015. pp. 93-122.

sorban a megfélemlítésre, a rettegésre és a pánikkeltésre koncentrált.¹⁰ Az alkalmazott erők, eszközök és módszerek tekintetében rendre végeláthatatlan gyűlöletet, rombolást és káoszt tapasztalhattunk. A 21. század tanúsága szerint a terrorizmus fegyveres támadásai – a csekély erő- és anyagi források kapcsán – az információs fölény elérése mellett elsősorban a lakosság megnyerésére és bevonására irányul. Ebből adódóan mára a Közel-Keleten folytatott fegyveres harc során jelentősen növelték a „közvetett műveleteknek” nevezhető eljárásokat. Ezek rendre indirekt és kognitív hatású, hálózatokban megjeleníthető, bármilyen plusz információtartalmú közlések, illetve szimbolikus értékkel bíró cselekmények (pl.: támadásokhoz kapcsolódó hekkelés, kiszivároztatás, mém-gyártás, közösségi megosztás). Az USA-ban és Európában végrehajtott terrortámadások esetében sajátos pszichológiai és információs hatásokat tapasztalhattuk.¹¹

A katonai területen kidolgozott és alkalmazott műveletek vizsgálatához stratégiákat, doktrínákat, műveleti eljárásokat, egyéb szabályzatokat találhatnak az érdeklődők. A hadtudomány ezen a területen az ellenséges cselekmények felderítésére, akadályozására, megelőzésére, illetve a hasonló információs tartalmú közdelem megvívására és megnyerésére már több kérdéskörben is adott katonai és sok esetben, polgári értelemben is sikeres válaszokat.¹²

A 2016. július 07-08-án a varsói NATO csúcson is kinyilvánításra került, hogy a számítógépes támadások veszélyt jelentenek a Szövetség biztonságára, amire ugyanolyan hatásuk lehet, mint a hagyományos fegyvereknek. Ezért a különböző katonai jellegű műveletek miatt a lehetséges légi, szárazföldi és tengeri hadszínterek mellett a kibertér is hadszíntérnek¹³ tekinthető.¹⁴ Az életet egyre több

¹⁰ Bővebben: KIS-BENEDEK József: *Dzsihadizmus, radikalizmus, terrorizmus*. Zrínyi Kiadó, 2016. p. 279.

¹¹ Bővebben: SIMON László: *A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására*. In: *Szakmai Szemle*, 2015. 2. sz. pp 145-162.

¹² MUNK Sándor: *Hadtudományi kutatók és kutatási területeik, 1. rész: A hadtudomány részterületeinek empirikus vizsgálata*. *Hadtudomány*, 2015. 1-2. sz., pp. 4-16.

¹³ „Hadszíntér: háromkiterjedésű földrajzi térség, amelyben a hadviselő (összeütköző) felek haderőiket összevonják, szétbontakoztatják, és egységes hadászati elgondolás és terv alapján haditevékenységet folytatnak.” ... „A haditechnikai fejlődés ma már problematikussá teszi a hadszínterek elhatárolását, mivel azok a szemben álló hadviselő felek országainak teljes mélységére kiterjedhetnek, valamint a kozmikus térségre is.” SZABÓ József (szerk.): *Hadtudományi lexikon*. 1. köt. 472. o.

¹⁴ „Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.” *Warsaw Summit Communiqué*, 70-71 pont.

számítógépes rendszer támogatja, amelyek kiesésének hatása – különös tekintettel a kritikus- infrastruktúrákra, információs infrastruktúrákra – fokozott kockázatot jelent a nemzetek számára.

Az információs műveletek tárgykörének ismerete segíti a terrorizmus indirekt hadviselésének stratégiai és lokális szintű megértését. A Magyar Honvédség 2014-ben kiadott információs műveletek doktrínája¹⁵ – a NATO AJP-3.10 doktrínában¹⁶ foglaltakkal megegyezően – az alábbi információs műveletek sorolja fel:

- Lélektani műveletek (angolul: Psychological Operations – PSYOPS);
- Megjelenés, viselkedés, arculat (a.: Presence, Posture, Profile – PPP);
- Műveleti biztonság (a.: Operational Security – OPSEC);
- Információs biztonság (a.: Information Security – INFOSEC);
- Megtévesztés (a.: Deception)
- Elektronikai hadviselés (a.: Electronic Warfare – EW)
- Fizikai megsemmisítés (a.: Physical Destruction – PD)
- Kulcsfontosságú vezetőkkel való érintkezés (a.: Key Leaders Engagement – KLE);
- Műveletek számítógépes hálózatokkal (a.: Computer Network Operations – CNO);
- Civil-katonai kapcsolatok (a.: CIMIC).

Rózsa Tibor 2016-os doktori értekezésében – hivatkozva többek között a technológia és a nemzeti haderők fejlettségi szintjeire – teljes áttekintést nyújt a műveletek taktikai szintű, lokális alkalmazhatóságáról. Kutatásai kapcsán kiemelte, hogy az információ katonai felhasználásának fejlődési iránya az indirekt hadviselés¹⁷ előretörésével, illetve annak stratégiai szintű alkalmazásával teljesezhet ki: *„Lényege, hogy a háború fő célkitűzései, illetve az elérni kívánt végállapot nemcsak a célpontok fizikai megsemmisítésével, hanem stratégiai hatások kiváltásával, többek között információs műveletek alkalmazásával is megvalósíthatók.*

http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber (Letöltés ideje: 2017. 07. 31.)

¹⁵ Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014.

¹⁶ AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3.

<http://info.publicintelligence.net/NATO-IO.pdf> (Letöltés ideje: 2017. 09. 15.)

¹⁷ Rózsa értekezésében csak a hagyományos hadviselést érinti, pedig az indirekt hadviselés a gerilla hadviselés hadikultúrájának is része. In: RÓZSA Tibor: Az információs műveletek alkalmazásának lehetőségei a Magyar Honvédség feladatrendszerében. NKE Doktori (PhD) Értekezés 2016, http://hhk.uni-nke.hu/uploads/media_items/rozs-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszerében.original.pdf (Letöltés ideje: 2017. 09. 15.)

Ebből adódóan a műveletek hatásalapú megközelítése a tervezett végállapot elérésére koncentrál és ennek szem előtt tartásával foglalja rendszerbe a műveletek tervezését, végrehajtását és értékelését.”¹⁸

A magyar katonai doktrína értelmezése szerint az információ „felhasználásával” kapcsolatos műveletek során – például a NATO-nak, egy ad-hoc szövetségnek, illetve adott nemzetnek (nemzeteknek) – a stratégiai célok elérése érdekében a képességeknek megfelelően összehangolt kommunikációs tevékenységet kell folytatnia magasabb műveleti szinteken is. A nemzeti feladatok végrehajtása során a stratégiai kommunikáció szintjén egységesen kell kezelni a nyilvános diplomácia, a tömegtájékoztatás, katonai és közkapcsolati tájékoztatás, valamint együttműködés, továbbá az információs műveletek és a lélektani műveletek egymásra ható eszközrendszerét.

Az országokban, így hazánkban is rendelkezésre álló számítógépes és infokommunikációs hálózatok ez alapján egy speciális műveleti környezetként értelmezhetők. Ebben a térben megjelenő káros (nem jogkövető) cselekményeket folytató egyéneket (csoportokat) így nemcsak bűnözőkként kell vizsgálnunk.

Az internet, mint média szerepe egyre növekszik. Az online hírek gyors terjedése, a különféle internetes hírportálok hírvadászata a megfélemlítéseknek hatékony, gyors forrása tud lenni, mindamellett, hogy az olvasókat befolyásolni tudják. A verseny a hírek mielőbbi megjelenítéséért sok esetben azt eredményezi, hogy a valóságtartalom ellenőrzése nem történik meg. Az internetes társadalom befolyásolása a híroldalakon keresztül az úgynevezett álhírekkel (hoax) is megvalósulhat, ami ugyanúgy képes a közvélemény befolyásolására a „virtuális fegyvertárban” szerepeltetve, mint a valós életben a robbanószerkek.

Az interneten folytatott befolyásolás már az országok választási rendszereiben is jelen van, amelyről egyre több hír¹⁹ kerül napvilágra. Ezen tevékenységek bizonyítása azonban nehéz, sokszor lehetetlen feladat.

A kibertér egyik sajátossága, hogy a felhasználók és közösségeik, így a terrorista szervezetek rejtett kommunikációt, információ megosztást tudnak folytatni rajta, olyanokat, amelyek felderítése rendkívül nehéz. Az adatok átvitelének ellenőrzése a túlmutat a közfelfogás szerinti hangfelismerés és a lehallgatások eddigi rendszerén. A védelem területén ki kell terjeszteni a gondolkodásunkat többek között az internetalapú hangkommunikációra, a titkosított csatornákra, a szteganográfiára, a különféle csetelési lehetőségekre is, amelyek akár a többszereplős internetes játékok üzenőfelületein is folynak.

A klasszikus pont-pont közötti információcseré (az egyszerű adó-csatornavető modell) valós és virtuális elemei, már nem egyértelműen azonosíthatók. A

¹⁸ Uo. pp. 35-36.

¹⁹ MTI: Orosz napilap mutatta be hogyan befolyásolták az amerikai választásokat 2017.10.17. In: www.Sg.hu, <https://sq.hu/cikkek/it-tech/127765/orosz-napilap-mutatta-be-hogyan-befolyasoltak-az-amerikai-valasztasokat> (Letöltés ideje: 2017.10.18.)

felhőszolgáltatások elterjedése további lehetőségek tárházát hozta elő a védendő információ rejtésének.

A kibertér felületet nyújt a terrorista szervezeteknek a toborzásokhoz. Széles körben tudják a világhálón rejtve és nyíltan is hozzáférhetővé tenni ideológiájukat, propaganda videóikat, amelyekkel bizonyos körülmények között élők sok esetben azonosulni tudnak. A kiképző táborokba az interneten történő toborzás hatására számos fiatal indul meg, akik sok esetben visszafordíthatatlan szélsőséges radikalizálódáson esnek át.

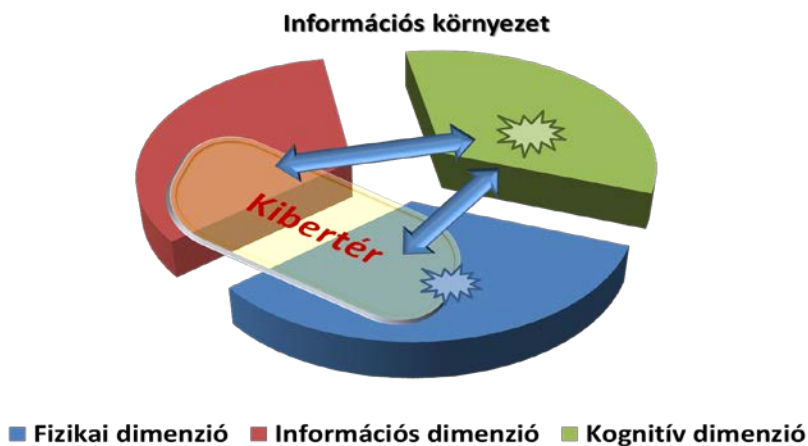
Az internetes felhasználók tömegei elől rejtett, illetve kevésbé ismert és használt deep (mély) WEB, dark (sötét) WEB lehetőséget nyújt a terrorszervezeteknek az illegális fegyverkereskedelemre, a különféle támadási technikák – például robbanószer előállításának – népszerűsítésére. A felderítés, védelemvalójában egy macska-egér játékhoz hasonló. A „jó” oldal az eseményeket követni, de a valós személyek felfedése rendkívül nehéz és költséges az interneten átmenő forgalom nagysága és a titkosító technológiák alkalmazása miatt. A hekker oldal képes a piacon szereplő eszközök, technológiák tesztelésére és a sérülékenységek felfedése után azok használatára, amely sok esetben „zero day” sérülékenységgként még hónapokig használható, azok felfedezéséig és a védekezési technika publikálásáig.

A kibertérben folytatott ellenséges tevékenységek, üzenetek megjelenítése során az elkövetői körben növekvő számba jelennek meg magukat dzsihadistáknak valló harcosokból álló közösségek. Nem csak bűnügyi szempontú, egyedi, illetve csoport-motiváció alapján, „szükségleteik kielégítése céljából” cselekszenek, hanem mint katonák, harcosok. Az ő esetükben a katonai többnemzeti megoldások során eddig alkalmazott módszerek kibővítése és elmélyítése lehet a megoldás. A kulturális felfogások sokszínűsége miatt ez egyre komplexebb és folyamatosan frissülő megközelítést igényel. Az eltérő motívumú elkövetők ellen folytatott kommunikációs és információs tevékenységeknek katonai értelemben koherensnek kell lennie. Kölcsönösen erősítenie kell egymást a résztvevőknek úgy, hogy a hordozott üzenetek minden szinten (pl.: politikai, katonai, stratégiai, regionális, helyi értelemben) egyeztetett, valamint a végrehajtásban közreműködő, „nem csak katonák” számára is érthető és egységes legyen.²⁰

A terrorizmus kapcsán jelentkező konfliktusok rendezésének, illetve az abból fakadó válságok kezelésének bonyolult rendszerében a katonai és nem katonai elemek kooperációját kell megvalósítani. Ezzel párhuzamosan az egymásra ható feladatok végrehajtásának egységes felfogása egyre bonyolultabb információs megközelítést, illetve tervezést igényel. A harcoló felek környezetét, a célokat és a célközönséget is egységként kell kezelnünk, mint a fegyveres küzdelmek esetében.

²⁰ Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014.

A legkülönbözőbb társadalmi, technikai, vagy akár ideológiai hálózatokba kapcsolt individuumok miatt nemcsak a fizikai erőszakkal, hanem az információ közvetlen hatásaival is foglalkoznunk kell. A földrajzi és a virtuális tér kapcsolata olyan „hadszíntér”, amelyben a kognitív tartomány támadhatóságának felértékelődésével kell szembe néznünk. Ebben a bennünket is körülvevő speciális információs környezetben a terrorszervezetek egyre növekvő hatékonyságot tudnak felmutatni. Az egyének bonyolult társadalmi, környezeti és technikai kapcsolatrendszere, valamint a közvetített üzenetek célba juttatása miatt az általunk már említett „közvetett műveletek” információ és hálózat-centrikussá váltak. A hálózatokat alkotó rendszerek támadása, illetve védelme – amely eddig leginkább technikai értelemben valósult meg – kibővül a kapcsolódó kognitív térben folytatható műveletekkel (1. ábra). Mivel a hálózatok működése a felhasználóik nélkül értelmüket veszítik, ezért mára az egyének biztonsága többjelentéssel bír. Ebben a hálózat alapú információs környezetben egyszerre és egymásra hatva vannak jelen a felhasználók, mint állam- és választópolgárok, illetve az életüket meghatározó állami és társadalmi szervezetek (pl.: kulturális, közlekedési, oktatási, gazdasági, humanitárius hálózatok), és nem utolsósorban az adott közösségek meghatározó szimbólumok is.



1. ábra: Az információs környezet (saját szerkesztés)

A kibertér a jelenlegi racionális felfogás szerint fizikai és információs dimenziójából áll. Az információs környezetben ezt egészíti ki a kognitív dimenzió. A kibertérben folytatott harcot a kiberhadviselés katonai értelmezése írja le: Az információs fölény részeként értelmezhető kiberfölény kivívása „az információs

*hadviselésen belül folytatott kiberhadviseléssel valósítható meg.*²¹ Már az értelmezés is azt mutatja, hogy a racionális megközelítésen túl, a kibertérben folytatott küzdelem nem csak a fizikai rendszerek pusztításáról, illetve katonai értelemben az ellenséges célpontok fizikai megsemmisítéséről szól. A fegyveres harc közvetlen hatásai mellett értékelésünk szerint megjelenik egy elvont, kognitív elem is, amely e küzdelem közvetett hatását is magába foglalja. A társadalom, a gazdaság, az oktatás, az egészségügy vagy például a közszolgáltatás egyes elemeinek, illetve a közösségek szimbólumainak összekapcsolt erőszakostámadása, pontosan a közvetett hatásaiban éri el a félelmeink növekedését. Az általunk közvetett támadásként értelmezhető műveleteket követően a fizikai állapot visszaállítása, a szabályok felülvizsgálata, illetve módosítása, valamint a védelem újrászervezése (egy új kórház, egy iskola vagy egy felhőkarcoló felépítése) az emberek biztonságérzetét már nem fogja tudni teljes mértékben visszaállítani. Jelenkori tapasztalatainkat a terrorizmus és az ellene folytatott küzdelem napról, napra bővíti. Az információk közvetett hatására válnak egyesek radikálissá és agresszívvá. Vannak olyanok, akik – közvetlen kapcsolat nélkül – az ISIS vagy az al-Kaida mint terrorjelenség nevében gyilkolnak. Teszik ezt úgy, hogy repülőgépeket vagy teherautókat használnak fel, amelyek hagyományos értelemben véve még fegyvernek sem minősülnek.

A kibertérben folytatott tevékenységek jogi kérdései

Az Európai Unió kiberbiztonsági stratégiája számos átfogó kérdéssel foglalkozik, melyek az alábbiak:

- „*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 számára, és az Unió alapértékeinek támogatása.*”²²

A fentieket figyelembe véve a stratégia csak védekező képességeket tartalmaz. A kibertámadás felvetése napirenden kívül esik, amelyet katonai értelemben – terrorista és extrémista szervezetekkel szembeni fellépés, aktív beavatkozások és válaszlépések nélkül – nehéz értelmezni.

²¹ HAIG Zsolt: *Információ, Társadalom, Biztonság. NKE Szolgáltató Kft, 2015. pp. 95.*

²² Az Európai Unió kiberbiztonsági stratégiája

<http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001> (Letöltés ideje: 2017. 09. 15.)

A kibertérben folyó műveleteket jogi aspektusból vizsgálva a támogatás megelőző csapással, aktív támadással történő esete jogszabályi oldalról nem definiált. Ez egyrészt abból adódik, hogy nehezen bizonyítható a kibertérben folyó tevékenység, a másik oldalról pedig a tevékenységek főleg a támadás megelőzésére, felderítésére vagy a kár elhárítására irányulnak. Ezért katonai értelemben gyakran kérdésként merül fel, hogy a kibervédelem támadás nélkül hozhat-e védelmi szempontból megfelelő eredményt, vagy szervezeti szinten kell felállítani olyan támadó képességet, amely egy esetleges rosszindulatú beavatkozás esetén képes a rendszereket ért támadás hatásának csökkentésére, esetlegesen a támadó fél semlegesítésére.

A nemzeti kiberbiztonsági stratégiában foglaltak szerint célként került rögzítésre, hogy Magyarország „*rendelkezzen hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességekkel a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen,*”²³ A tevékenységek itt is védelmi jellegűek, az aktív védelem említése nélkül.

A honvédelmi miniszter éves értékelő és feladatszabó vezetői értekezlete előkészítésének és végrehajtásának feladatairól szóló 84/2014. (XII. 23.) HM utasításban már megjelent jogszabályi oldalról a kibertérből származó információszerző képesség (Cyber Intelligence) fejlesztése, amely nem összetéveszthető a nyílt forrású információszerzéssel (Open Source Intelligence).

Kibertérben jelentkező események megelőzése érdekében eseménykezelő központok üzemelnek nemzetközi együttműködésben,²⁴ melyek feladata a tájékoztatások, riasztások megtétele mellett az eseménykezelések, hatósági feladatok ellátása. Az úgynevezett CERT-ek szerepe a jövőben tovább növekszik az internet alapú technológiák, a dolgok internete (IoT) terjedésével párhuzamosan.

A nem katonai értelmű támadó szándék a Büntető Törvénykönyvről szóló 2012. évi C. törvényben megjelenik az információs rendszer vagy adat megsértése fejezetben, amelyben definiálásra kerül az információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belépés szankciója.²⁵

A katonai oldal kihívásai

A kibertér a hagyományos hadszínterekhez képest jelentős különbséget mutat. A virtuális térben való jelenlét teljesen más felkészültséget igényel, mint akár a

²³ Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat.

²⁴ Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.

²⁵ A Büntető Törvénykönyvről szóló 2012. évi C. törvény 423. §164 (1).

szárazföldi, légi, vagy a haditengerészeti területen. A „kiberkatonák” esetében a „túlélés” legkevesbé a fizikai képességeken mutatkozik meg, az informatikai tudás, az általuk használt célszoftverek és eljárások ismerete esetükben a meghatározó. A fizikai követelmények teljesítése sok, a feladatnak és beosztásnak megfelelő jelöltet rostál ki.

Kihívásként jelentkezik a kimagasló tudással rendelkező informatikusok felvétele és katonai pályán tartása, mivel a civil életben a keresetük többszörösét érhetik el és a kötött jogszabályok a külsős fizetések szintjéig történő eltérítést nem teszik lehetővé.

A pályán tartást nehezítik, hogy folyamatos képzések lennének szükségesek a megfelelő hatékonyság eléréséhez, azonban azok igen költségesek és tovább növelik a katonai tudásának piaci versenyképességét. Így csak a legnagyobb hivatástudattal rendelkezők informatikusok maradnak a szervezetek keretein belül. A megfelelő képzések biztosítják a szoftver kritikus biztonsági hibák, biztonságos programozás elsajátítását.

Észtország példájára az önkéntes kibervédelmi tartalékos rendszer²⁶ megoldást nyújthat a kiberterroristák által végrehajtott műveletek elhárításához, illetve a szükséges ellenreakciók megtételéhez, azonban ez komoly tervező feladatot igényel. Az önkéntes tartalékos kibervédelmi egység létrehozásának indokait Krasznai Csaba 2011-ben már összefoglalta.²⁷

A kibertámadások ugyanúgy veszélyeztetik a kritikus információs rendszereket, mint ahogy a katonai műveleteket is. Célzott támadásokkal a haderő béke és tábori rendszereit is veszélyeztethetik a terrorista szervezetek kibercsoportjai. A kiszivárgott kiberfegyverek, vagy a napjainkban egyre gyakoribb zsarolóvírusok és kampányaik valós veszély hordoznak. Kassai Károly véleménye szerint a „kibervédelem” területű gondolkodás a honvédelmi szakterületen a miniszteri utasításban meghatározott információbiztonsági politika komplex továbbfejlesztését jelenti. A kihívások a következő területekre csoportosíthatók:

- szabályozási környezet kialakítása (érintett szervezetek hatáskörének, feladatainak kijelölése, beleértve a különleges jogrend speciális esetét);
- az elektronikus adatkezelő hálózatok biztonsági szintjének emelése (technikai jellegű feladatok);
- kibertámadások elleni képességfejlesztés (az elektronikus

²⁶ KASKA, Kadri - OSULA, Anna-Maria, - STINISSEN Jan: *The Cyber Defence Unit of the Estonian Defence League*, Tallinn 2013.
https://ccdc.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (Letöltés ideje: 2017. 09. 15.)

²⁷ KRASZNAI Csaba: *A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai*. ZMNE 2011. (PhD értekezés)
http://krasznay.hu/presentation/szerzoi_ismerteto_krasznay.pdf (Letöltés ideje: 2017. 09. 15.)

eseménykezelés és az elektronikus információvédelmi feladatok felügyeleti kérdései);

- a szaktudás növelése (felhasználók és üzemeltetők szerint specializált képzések, beleértve a kibervédelmi gyakorlatok kérdését is);
- kutatás és fejlesztés (nemzeti és nemzetközi szintű lehetőségek felhasználása);
- együttműködés (egyszerűen megfogalmazva: akivel csak a kétoldalú előnyök mentén az elképzelhető).²⁸

Következtetés

Az országok és emberi közösségeik eltérő erőforrása, stratégiai és taktikai elképzelése, továbbá a kulturális és többek között vallási sokszínűsége számos eddig ismeretlen folyamatot eredményezett. A már említett infokommunikációs hálózatok segítségével a média élre tört az emberek tájékoztatása terén, és bemutatta a tudás „Janus-arca” mellett a távoli konfliktusok, szélsőségek és erőszak sokak számára értelmezhetetlen valóságát. A posztmodern társadalmak korára az európai polgárok, mint individuumok („biztonsági objektumok”) mindennapjait egyre inkább a hálózatokban áramló adatok és információk megismerése, megosztása, illetve birtoklása határozta meg.

A kibertér, mint új hadszíntér számos feladat elé állítja a jövő katonai gondolkodását. Az információs műveletek komplexitása képességek felállítását, erősítését igénylik. A kibertérben folytatott műveletekhez szükséges technikai és humán erőforrás igényeket fel kell mérni és tudatosan ki kell alakítani.

Felhasznált irodalom

- 1139/2013. (III. 21.) Korm. határozat - Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 2013. évi L. törvény - az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2012. évi C. törvény - a Büntető Törvénykönyvről szóló
- BERÉNYI Dénes: *Hogy látja ma egy fizikus a világot?* (2010) <http://vigilia.hu/regihonlap/2010/7/berenyi.html> (Letöltés ideje: 2017. 09. 15.)
- BOROS János: Jean-François Lyotard, a különbözőség elgondolója, Kísérlet egy tudáselméleti megközelítésre, *Jelenkor: Irodalmi és Művészeti Folyóirat*, XLII. évf. 3.sz. 1999. pp. 298-306. ISSN 1588-0885

²⁸ KASSAI Károly: *Kibervédelem és a Magyar Honvédség. Hadmérnök, VII. évfolyam, 4. szám, p. 137-138.*

- HAIG Zsolt: Információ, Társadalom, Biztonság, NKE Szolgáltató Kft, 2015. pp. 93-122. ISBN 978 615 5527 08 1
- KASKA, Kadri - OSULA, Anna-Maria, - STINISSEN Jan: The Cyber Defence Unit of the Estonian Defence League, Tallinn 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (Letöltés ideje: 2017. 09. 15.)
- KASSAI Károly: Kibervédelem és a Magyar Honvédség, Hadmérnök, VII. évfolyam, 4. szám, p. 137-138.
- KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus, Zrínyi Kiadó, 2016. p. 279. ISBN 978 963 327 739 3
- MUNK Sándor: Hadtudományi kutatók és kutatási területeik, 1. rész: A hadtudomány részterületeinek empirikus vizsgálata, Hadtudomány, 2015. 1-2. sz., pp. 4-16. ISSN 1215 4121
- RESPERGER István - KISS Álmos Péter - SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban – Kis háborúk nagy hatással Zrínyi Kiadó, 2014. pp. 13-44. ISBN 978 963 327 592 4
- RÓZSA Tibor: Az információs műveletek alkalmazásának lehetőségei a Magyar Honvédség
- SIMON László: A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására, In: Szakmai Szemle, 2015. 2. sz. pp 145-162. ISSN 1785-1181
- SIMON László: Az információ mint fegyver? In: Szakmai Szemle 2016. 1. sz. pp. 34-60. ISSN 1785-1181
- SZABÓ József (szerk.): Hadtudományi lexikon. 1. köt. Magyar Hadtudományi Társaság, Budapest, 1995. ISBN 0469000676354
- Sz.n.: AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3. <http://info.publicintelligence.net/NATO-IO.pdf> (Letöltés ideje: 2017. 09. 15.)
- Sz.n.: Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014. feladatrendszerében, NKE Doktori (PhD) Értekezés 2016, http://hhk.uni-nke.hu/uploads/media_items/rozsa-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszerében.original.pdf (Letöltés ideje: 2017. 09. 15.)
- Sz.n.: Az Európai Unió kiberbiztonsági stratégiája. <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001> (Letöltés ideje: 2017. 09. 15.)
- Sz.n.: Orosz napilap mutatta be hogyan befolyásolták az amerikai választásokat. MTI. 2017.10.17., <https://sg.hu/cikkek/it-tech/127765/orosz-napilap-mutatta-be-hogyan-befolyasoltak-az-amerikai-valasztasokat> (Letöltés ideje: 2017.10.18.)