HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

VI. Évfolyam 4. szám 2011. december

ZMNE
BUDAPEST

A szerkesztőség elérhetősége:
Zrínyi Miklós Nemzetvédelmi Egyetem, 1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet
Postacím: 1581. Budapest Pf.:15.
Telefon: +36-1-432-9048
Fax: +36-1-432-9208
HM: 29-734
e-mail: hadmernok@zmne.hu
web: http://hadmernok.hu

Kiadó: Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE)
Kiadásért felelős: Prof. Dr. Padányi József, a ZMNE mb. rektora
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Dr. Balajti István

Dr. Berek Tamás mk. őrnagy – ZMNE egyetemi docens

Dr. Bottyán Zsolt mk. százados – ZMNE egyetemi docens

Prof. Dr. Bukovics István – Wesley János Főiskola

Bunyitai Ákos – ZMNE KMDI doktorandusz

Csépainé Széll Pálma – ZMNE

Dávidovits Zsuzsanna – ZMNE KMDI doktorandusz

Dr. Fáy Gyula – Wesley János Főiskola

Dr. Földi László mk. alezredes – ZMNE egyetemi docens

Gyarmati Gábor őrnagy – ZMNE KMDI doktorandusz

Dr. habil. Horváth Attila alezredes – ZMNE egyetemi docens

Dr. Hornyacsek Júlia őrnagy – ZMNE egyetemi adjunktus

Horvayné Fehér Judit – ZMNE KMDI doktorandusz

Dr. Huszár András ny. r. ezredes – Pécsi Tudományegyetem, Általános Orvosi Kar, Igazságügyi Orvostani Intézet

Inkovics Ferenc – ZMNE KMDI doktorandusz

Kormos Tímea – Miskolci Egyetem Állam- és Jogtudományi Kar, jogász szak

Kovács Zoltán ezredes – Nemzetbiztonsági Szakszolgálat

Kozma Zsolt – Igazságügyi Szakértői és Kutatóintézetek, Kaposvári Intézet

Dr. Kun István – Wesley János Főiskola

Lasz György – ZMNE KMDI doktorandusz

Dr. Muha Lajos mk. alezredes – ZMNE főiskolai tanár

Prof. Dr. Munk Sándor ny. mk. ezredes – ZMNE egyetemi tanár

Pápai Tibor őrnagy – MH Honvédkórház - Sürgősségi Centrum – centrumvezető ápoló, Semmelweis Egyetem Egészségtudományi Kar Oxiológia és Sürgősségi Ellátás Tanszék - adjunktus

Pataki János – ZMNE HDI doktorandusz

Papp Zoltán őrnagy – ZMNE KMDI doktorandusz

Prekup Zsolt – ZMNE KMDI doktorandusz

Szabó András Miklós – ZMNE KMDI doktorandusz

Serege Gábor főhadnagy – ZMNE KMDI doktorandusz

Dr. Sulányi Péter – Suprex kft.

Tibenszkyné Dr. Fórika Krisztina százados – ZMNE egyetemi docens

Tóth Georgina Nóra – ZMNE KMDI doktorandusz

Tóth György – Országos Mentőszolgálat Észak-Alföldi Regionális Mentőszervezet

Venekei József alezredes – ZMNE egyetemi adjunktus

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Berek Tamás
berek.tamas@uni-nke.hu

VAGYONVÉDELMI KONCEPCIÓ KIALAKÍTÁSÁNAK SAJÁTOSSÁGAI VESZÉLYES ANYAGOK VIZSGÁLATÁT BIZTOSÍTÓ LÉTESÍTMÉNYEK ESETÉBEN

Absztrakt

A vagyonvédelmi koncepció kialakítását követően a komplex biztonsági rendszer tervezésekor komoly elemző és értékelő munkát követel meg a védelmi alrendszerek helyes arányainak kialakítása. Egy olyan laboratóriumban, ahol veszélyes anyagot, radioaktív izotópokat tárolnak és használnak fel és ionizáló sugárzás, valamint mérgezés veszélyével járó munkakörben, a vagyonvédelem mellett fontos a biztonsági rendszabályok betartása is. A szerző bemutatja, hogy a vagyonvédelmi komplexum elektronikus komponensének kialakításakor milyen sajátosságokat kell figyelembe venni a veszélyes anyagok biztonsági kockázata okán.

In order to configurate a safeguarding conception, we have to create a complex security system. We have to make a plan, the plan has to be analised and interpreted. We have to configurate the right propotion of the defend systems. In laboratories, where hazardous materials, radioactive isotopes are stored and used for a job under the risk of poisoning and ionizing radiation, it is important to compliance with the safety regulations. The author demonstrates that what kind of specialties have we take into consideration for the reason of the hazardous materials.

Kulcsszavak: *CBRN fenyegetés, biztonsági környezet, beléptető rendszer ~ CBRN threat, security environment, access control system*

A BIZTONSÁGI HÁTTÉR

A Nemzetközi Atomenergia Ügynökség (NAÜ)(IAEA) 2009-es kimutatása szerint 1993 és 2008 között 1562 radioaktív anyaggal kapcsolatos esetet jelentettek, melyek közül 336 esemény jogosulatlan birtoklás és az ahhoz kapcsolódó bűncselekmény, 421 esemény bizonyítottan lopás vagy elvesztés, és 724 incidens egyéb jogosulatlan tevékenység volt.[1]

Csak 2009 július és 2010 júniusa között jelentett 222 incidens közül 21 jogosulatlan birtoklás és az ahhoz kapcsolódó bűncselekmény, 61 lopás vagy elvesztés és 140 egyéb, nem engedélyezett tevékenység volt megállapítható. Ezen időszak alatt öt incidenst jelentettek dúsított uránnal vagy plutóniummal kapcsolatban, amelyek közül egy volt jogellenes birtoklás, a többi négy egyéb jogosulatlan tevékenységnek bizonyult. [2]

A jelentett lopások és elvesztések elsősorban többek között olyan radioaktív forrásokat érintettek - 137-Cs, 241-Am, 90-Sr, 60-Co,192-Ir - melyek azt mutatják, hogy a források általában hordozható ipari berendezések, melyek mobilizálhatóságuk miatt fokozottan ki vannak téve egyébként is eltulajdonítás, vagy elvesztés kockázatának. Ez azt vetíti előre, hogy javítani kell a biztonsági intézkedések és eljárások hatékonyságát a jövőben. A tolvajokat gyakran nem az eszközben található sugárforrás felhasználhatósága vagy értékesíthetősége, hanem a berendezés feketepiaci eladhatósága, esetleg az eszköz fémtömege csábítja. Az esetek többségében csupán kis mennyiségű radioaktív anyag csempészete történt, amely ugyan nukleáris fegyver készítésére nem, de radiológiai diszperziós eszköz készítésének alapjául szolgálhat.

A NAÜ Kormányzótanácsa által 2002 márciusában jóváhagyott egy, a nukleáris terrorizmus elleni védelemre irányuló tevékenységterv (GOV/2002/10) kitér többek között a használatban levő, tárolás vagy szállítás alatt álló nukleáris és egyéb radioaktív anyagok ellenőrzéseinek szabályozására, elszámolhatóságára és védelmére. A tevékenységterv kiterjed arra is, hogy amennyiben az anyagok előfordulási helyükön jelenleg még nem állnak védelem alatt, az anyagok jogtalan eltulajdonításának, illetve az azok csempészetére irányuló kísérleteknek a felderítésére intézkedéseket kell bevezetni. A fenti probléma kezelésének indíttatásából az EU Tanács 2003. december 22-én elfogadta a nagy aktivitású zárt sugárforrások és a gazdátlan sugárforrások ellenőrzéséről szóló 2003/122/Euratom irányelvet, melynek többek között célkitűzése minden nagy aktivitású sugárforrás nyilvántartásba vétele és ellenőrzése a tárolási helyével együtt.

2005 júliusában a részes államok és az Európai Atomenergia Közösség megállapodott a „nukleáris anyagok fizikai védelméről szóló egyezmény (CPPNM)” módosításáról, kiterjesztve annak hatályát a polgári célú belföldi felhasználású, tárolás, valamint szállítás alatt álló nukleáris anyagokra és létesítményekre. Lényeges elvárás fogalmazódik meg ezzel egyidejűleg a részes államok irányában az ezzel kapcsolatos jogsértések büntetőjogi szankcionálásának tekintetében.

Fontos cél ezért a nem nukleáris, hanem orvosi vagy ipari célra alkalmazott sugárforrások –melyek némelyike nagyaktivitású– védelme, illetéktelen kezekbe kerülve bűnös céllal ugyanis felhasználhatók improvizált radiológiai diszperziós eszközök (IRDE) tölteteként terrorcselekmények elkövetésére. [3] A nukleáris biztonsági feladatok keretében az egyes országokban értékelik a nukleáris és egyéb radioaktív anyagok fizikai védelmének helyzetét, és azoknak a nukleáris vagy kutató létesítményeknek, illetve helyszíneknek a védelmét, ahol ezeket az anyagokat használják, vagy tárolják.

Megfogalmazódik a szakértők részéről ugyanakkor a CBRN fenyegetés más forrása miatti aggodalom is. A molekuláris biológiai, illetve a genetikai kutatások óriási léptékű fejlődése, illetve annak igénye nyomán új, magas biztonsági fokozatú laboratóriumok számának jelentős

növekedése figyelhető meg. Azok, amelyek hiányosságokat mutatnak a megfelelő biológiai biztonsági és biológiai védelmi előírások betartása terén potenciális veszélyforrást jelentenek.

Az utóbbi években számos ország – köztük olyan országok is, amelyek korlátozott mennyiségű erőforrással rendelkeznek – pénzeszközöket különített el magas biztonsági fokozatú laboratóriumok kialakítására. Ez egyfelől több kutató számára lehetővé teszi saját országában a kutatást olyan veszélyes kórokozókkal (pl. SARS koronavírus, vérzéses lázat okozó vírusok) melyekkel végzett kutatásokhoz való hozzáférés korábban korlátozott és nehézkes volt, másfelől azonban kockázatot is hordoz magában azokban az országokban, amelyek nem tudnak gondoskodni – elsősorban financiális okokra visszavezetve – a veszélyes létesítmények hosszú távú fenntartásáról, és/vagy nem nyújtanak megfelelő laborbiztonsági képzést az alkalmazottak számára. [4]

A BIZTONSÁGI RENDSZER KIALAKÍTÁSÁNAK NÉHÁNY SZEMPONTJA

Az előzőekben ismertetett biztonsági fenyegetések csökkentését célzó intézkedések hangsúlyozottan fontos eleme a különböző – bűnös céllal is felhasználható –veszélyes anyagok fizikai védelme. Veszélyes anyagot rejtő létesítmény, például veszélyes anyagok azonosításának feladatát ellátó laboratórium - melyben annak rendeltetésének megfelelően különböző műveleteket kell végezni veszélyes anyagokkal (radioaktív, vegyi, biológiai) vagy éppen azok azonosítását kell végrehajtani – védelmének kialakításakor néhány sajátosságot feltétlenül figyelembe kell venni.

A biztonsági rendszer felépítése érdekében kialakított védelmi filozófia alapjául szolgál a biztonsági kockázatelemzés, melynek ki kell térnie a laboratóriumban felhasznált veszélyes mérgező és radioaktív anyagok külső környezetbe történő kerülésére, gondatlan-, vagy bűnös szándék, vagy akár technológiai hiba közrehatásának eredményeként. [5]

A biztonságvédelmi program felépítésekor a jellemző összetevők - védelmi politika, fizikai védelem, információ-védelem, emberi tényező – alapfeltételeinek vizsgálata és kialakítása döntő fontosságú.

A vizsgálati (laboratóriumi) tevékenységből és a környezetéből eredő veszélyeztetettség feltárása és elemzése során meg kell állapítani a védelem célját, tárgyát, meg kell határozni a veszély forrásait, és ezek ismeretében kell megtervezni és kiépíteni a védelmi rendszert, úgy, hogy tételesen kell megjelölni a védendő értékeket és tevékenységeket.

A veszélyes anyagok vizsgálatának helyszínéül szolgáló létesítmény védelmét biztosító vagyonvédelmi rendszer tervezése szempontjából lényeges a későbbi feladat-végrehajtás helyszínének megelőző tanulmányozása, majd ezt követően a felmért paraméterek teljes körű kiértékelése.

A kockázatelemzés célja az adott létesítménnyel, üzemeltetésével és a benne folyó tevékenységekkel kapcsolatban esetleg előforduló lehetséges kockázatok azonosítása, csoportosítása és értékelése. Az elemzés során a kockázatok bekövetkezési valószínűségét, okozott hatását, illetve a kockázat bekövetkeztének elkerülését, illetve hatásának csökkentését lehetővé tevő intézkedéseket vizsgáljuk. Az elemzés során többek között az alábbi tényezőket kell figyelembe venni:

- A létesítmény környezeti adottságai, a környék bűnözési statisztikája.
- A létesítmény építészeti, energetikai, elektronikai, informatikai, stb. alrendszerei.
- A létesítmény üzemeltetési rendszerei, szabályzatok, hatósági előírások.
- A létesítmény alapfunkciói, időszakos, kiegészítő funkciók.
- A létesítményben dolgozó, oda látogató személyek összetétele.
- Biztosítási szerződések, feltételek. [6]

A környék bűnügyi fertőzöttsége. A veszélyes anyagokkal kapcsolatos tevékenység (vizsgálat, analízis) helyszínének szemléjével együtt értékelni kell annak - a védelem szempontjából meghatározó fizikai környezetét, az azt alkotó lényeges terepelemek számbavételével együtt.

A védelmi koncepció kialakításához azonban még számos adatra szükség van, többek között a terület bűnügyi helyzetére vonatkozóan. Ebben a szakaszban azt a kérdéskört kell tisztázni elsősorban, hogy a vagyonellenes cselekmények közül melyek fordulnak elő jellemzően (lopás, betöréses lopás, rablás, rongálás, szabotázs), ezen belül középületek, ipartelepek, építkezések, magánházak elleni, események gyakoriságát és azon elkövetések módszereit.

A bűnügyi helyzet-felmérés és tájékozódás fontos a biztonsági rendszer minimálisan szükséges védelmi kapacitásának meghatározásánál, s bár nem minden esetben lehet törvényszerű összefüggést kimutatni az adott környék bűnügyi szennyezettsége és a leendő projekt vagyonellenes cselekményei között, a megszerzett információk mégis stratégiai jelentőséggel bírnak a biztonsági terv elkészítésénél.

Az épületbe szerelt anyagok (technikai eszközök, különleges építő anyagok felhasználása, speciális technológia telepítése stb.) minősége és mennyisége szintén meghatározza a védelem kialakítását, a biztonsági szolgálat biztosítási tervét és majdani jóváhagyott működési szabályzatát. Nem elegendő a helyszínt biztosítani és megvédeni az esetleges elkövetőktől, a veszélyes anyagok vizsgálatát végzők és a végzett tevékenység folyamatos védelmére is legalább ugyanannyi erőt, ha nem többet kell fordítani. [7]

A labor mérete és elhelyezkedése a környezetében döntő jelentőségű, melynek előzetes értékelésére ugyancsak sort kell keríteni, melynek során ki kell mutatni azokat a kiemelten védendő épület-elemeket, amelyek hiányos védelem esetén könnyű támadási felületet nyújtanak az elkövetők számára. Az objektum mérete és elhelyezkedése annak okán is kiemelt jelentőséggel bír, hogy a létesítményben helyt foglaló veszélyes terek, anyagtároló területek elhelyezkedése szintén meghatározó a védelem szervezése szempontjából.

A létesítményben végzett tevékenység elemzése szintén meghatározó. Egy veszélyes anyagok vizsgálatával foglalkozó laboratóriumban, az ott végzett tevékenység veszélyes radioaktív, mérgező, esetleg fertőző anyagok esetenként mérgező harcanyagok szükségszerű felhasználásával történik. A laborkomplexumban kialakított ellenőrzött munkaterületek és munkafolyamatok ideértve az azokban résztvevő személyi állomány és a veszélyes anyagok, valamint a hulladékok tároló-helyiségei védelme kiemelt fontosságú. Nem kisebb súllyal igénylik a védelmet a munkaterületnek nem minősülő terek és laboratórium külső környezete.

A veszélyes anyagokkal történő üzemszerűen végzett tevékenység helyszínén tehát kockázatbecslést kell végezni, melyben az egyik kockázat egy törvénytelen cselekedet sikeres véghezvitelének megvalósítási valószínűsége. Ennek felméréséhez elengedhetetlen a cél sérülékenységének és a veszély mértékének ismerete, melyet célszerű írásba foglalni. [8]

Teljes védelmi koncepció kidolgozása

A védelmi koncepció gondos felépítése egy lényeges és kritikus állomása a vagyonvédelmi komplexum kialakítása során, hiszen a tervezési folyamat további szakaszait ez alapozza meg.

A védelmi koncepció a vagyonvédelmi rendszer egyes összetevőinek funkcióit, kapcsolatát, működési módját írja le. Meghatározza a szükséges mechanikai, elektronikai, információ-technológiai védelmi alrendszerek, eszközök főbb paramétereit, egymásra-épülésüket, funkcionális jellemzőiket, kezelésük, karbantartásuk módját.[6]

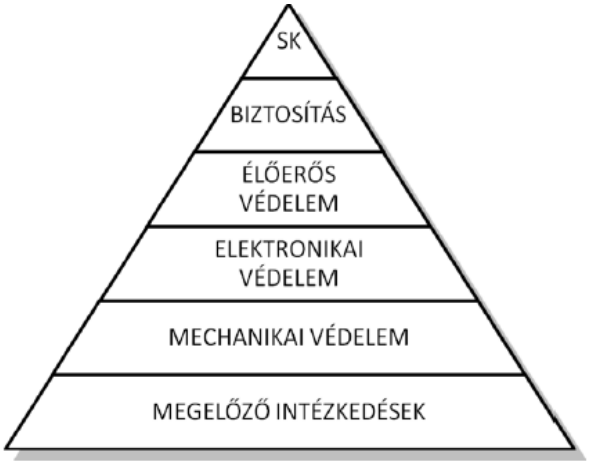
A védelem tervezésekor és kialakításakor az ellenőrzött térben a technológiai, a mechanikai - elektronikai - személyi biztonság magas színvonalú biztosítása érdekében a tervezett biztonságtechnikai alrendszereknek a laboratórium rendeltetésével összhangban történő kialakítása az egyik elsődleges szempont. Ahhoz, hogy a védelem folyamatos és átfogó legyen, a biztonságtechnikai rendszer felépítésnél az egyes, egymástól független, autonóm működésű alrendszerek hatékonyságot fokozó komplex összehangolására és a felügyelet feltételeinek biztosítására van szükség. A fizikai őrzés hatékonyságát biztosítja a mechanikai és elektronikus eszközök valamint az élőerős eljárások hatékony kombinációja, nem is beszélve a megelőző intézkedések szerepéről. A tevékenység rendjét meghatározó létesítményi biztonsági szabályzat az egyik lényeges alapdokumentum, melyet pontosan tanulmányozni kell a védelem tervezésekor. Az integrált védelem nem csupán azt jelenti, hogy a mechanikai védelmet technikai megfigyelésnek kell kiegészíteni. Szükséges egyfelől egy olyan biztonsági rendszer kiépítése, amelyben a beintegrált alrendszerek autonóm működésének feltételeit biztosító felügyeleti algoritmus összehangolja azok kommunikációját, ugyanakkor biztosítja a személyi felügyelet beavatkozási lehetőségét is, annak az objektum személyi állományának hatáskörében történő összpontosításával.

A laborkomplexum számára olyan épületfelügyeleti rendszer kiépítése szükséges, amely működése közben az emberi beavatkozás igénye hibaelhárítás, illetve egyes előre meghatározott kivételes biztonságot fenyegető helyzetekben merül fel.

A laborkomplexumban megfelelően elhelyezett érzékelők által generált jelzés az őrség diszpécser helyiségben is meg kell, hogy jelenjen természetesen, azonban a behatolásjelző-rendszerek élesítésének hatástalanításának valamint a veszélyes anyagok jelenlétét monitorozó alrendszer riasztóegységekkel egybeépített detektorai jelzéseinek nyugtázása és azokhoz kapcsolható intézkedési jogosultságok a laboratórium szakmai személyi felügyelete hatáskörében kell, hogy maradjanak.

A vagyonvédelmi alrendszer mindenkori működésére vonatkozóan az objektum biztonsági felépítésének megfelelően szükséges egy általános és különleges esetekre vonatkozó intézkedési terv készítése az élőerős védelmet megtestesítő biztonsági őrszolgálat részére, mely a kiépülő technikai rendszeren alapulva folyamatosan fejlődik. Ez alapján tud az őrség rendkívüli eseményekre (jogellenes cselekmény, tűz stb.) gyorsan és hatékonyan reagálni úgy, hogy a beavatkozásuk ne járjon egészségkárosodással az adott laboratórium alaprendeltetéséből fakadó veszélyforrásokat figyelembe véve. A vagyonvédelmi szolgálat járőreinek kiképzése és továbbképzése szükséges tehát akár a saját munkahelyi biztonságuk, akár hatékonyság szempontjából is vizsgáljuk.

Egy laborkomplexum biztonságánál az elektronikus vagyonvédelemi paletta szinte összes rendszere szóba jöhet: behatolásjelző, tűzjelző, oltó, gázjelző, beléptető, videó megfigyelő, hangosítási rendszer.



1. ábra. A komplex vagyonvédelem összetevői[1]
Forrás: Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései doktori (PhD) értekezés, 2009.

A tervezés során ki kell jelölni azokat a területeket, melyeket a veszélyforrások ismeretében fokozott védelemben kell részesíteni külön belépési jogosultsággal. A laborlétesítmények veszélyes tereinek védelmének biztosításakor kevés lehetőség nyílik az élőerős feladat ellátására ezért fokozni kell az elektronikus védelmi eszközök arányát és előtérbe kerülnek ugyanakkor a belső ellenőrzés megszilárdítására tett intézkedések. A laborszemélyzet feladata érvényesíteni a szabályokat és eljárásokat, kezelni és működtetni biztonsági rendszereket. Az közismert, hogy a vagyonvédelmi rendszer hatékonyságát a leggyengébb elemének hatékonysága determinálja. Nem kellő körültekintéssel felépített rendszereknek gyakorta az élőerős összetevője jelenti a leggyengébb láncszemet. A létesítményi biztonság fenntartása érdekében a felelősségi körök behatárolása mellett az ellenőrizhetőség biztosítása, illetve annak egyik feltételeként a szabályozási rendszer kialakítása elengedhetetlen többek között szabálytalanság, mulasztás, belső szabotázs esetén, a felelősség megállapításához és annak személyhez kötöttség biztosításához.

Az elektronikai védelem már önmagában komplex fogalom, több, önállóan telepíthető, önálló funkciókat ellátó biztonságtechnikai alrendszert foglal magába, úgy, mint: behatolás jelző-, beléptető-, videó felügyeleti-, áruvédelmi-, járőrkövető-, és tűzjelző rendszert. A behatolás jelző rendszerek elsődleges célja az élőerős védelem értesítése az illetéktelen behatolásról, behatolási kísérletről. A megfelelően tervezett és telepített rendszer, a mechanikai védelem eszközeire közvetlenül ráépülő érzékelői segítségével már a mechanikai védelem megsértésének kezdetén helyszíni hang- és fényjelzőkkel, illetve távjelzéssel - a távfelügyeleti központon keresztül, vagy közvetlenül - értesíti az élőerős védelmet. [6]

A fentiek szerint az alábbi elektronikai rendszerek alkalmazása szükséges az érintett létesítményekben:

- Behatolás- és támadásjelző rendszer,
- Videó figyelő és rögzítő rendszer,
- Beléptető rendszer,
- Elektronikus tűzjelző rendszer,
- Veszélyes anyagok jelenlétét monitorozó rendszerek

[1] A piramis csúcsán álló SK a „saját kockázat” rövidítése

Biztonság szerinti fokozatba sorolás

A behatolás jelző rendszerekre vonatkozóan a tervezési irányelveket az MSZ EN 50131-1 a „Riasztórendszerek. Behatolás- és támadásjelző rendszerek. Rendszerkövetelmények" szabvány határozza meg. A szabvány a behatolás- és támadásjelző rendszereket és részegységeiket az elérni kívánt biztonsági szintnek megfelelő biztonsági fokozatokba sorolja. A biztonsági fokozatok a kockázati szinteken alapulnak, melyet alapvetően az adott létesítmény típusa, az ott elhelyezett értékek és a tipikusan várható fenyegetés szintje határoz meg. A szabvány a fenti szempontok szerint négy biztonsági fokozatba sorolja az elektronikus vagyonvédelem eszközeit. Az alacsony kockázatú, 1. biztonsági fokozattól – amely korlátozott a behatolás-védelmi ismeretekkel és könnyen beszerezhető egyszerű kézi szerszámokkal rendelkező behatoló kockázatával számol- a magas kockázatú 4. biztonsági fokozatig – amely szakértelemmel és speciális szerszámokkal rendelkező behatoló támadását feltételezi.

Veszélyes anyagokat vizsgáló laboratóriumok vagyonvédelmi biztosítása céljából alkalmazott behatolás-jelző rendszernek a 3. - vagy a 4. biztonsági fokozatnak kell megfelelnie.

3. fokozat: Közepes és magas közötti kockázat A behatoló vagy a rabló vélhetően jártas a behatolás- és támadásjelző rendszerekben, és a szerszámok, hordozható elektronikus készülékek széles körű választékával rendelkezik

4. fokozat: Magas kockázat Akkor alkalmazandó, ha a biztonság minden más tényezőnél előbbre való. A behatoló vagy rabló vélhetően képes részletesen megtervezni egy behatolást vagy rablást, rendelkezik ehhez erőforrásokkal, és rendelkezik a berendezések teljes skálájával, beleértve olyan eszközöket is, amelyekkel a behatolás- és támadásjelző rendszer alapvető fontosságú részegységeit helyettesítheti." [9]

Szabotázs elleni védelem tekintetében a szabvány úgy fogalmaz, hogy*: „*A behatolás- és támadásjelző rendszer részegységeit el kell látni olyan eszközzel, amely meggátolja a belső elemekhez való hozzáférést, a szabotázs kockázatának minimalizálása céljából. A szabotázsvédelemre vonatkozó követelmények változhatnak a behatolás- és támadásjelző rendszer biztonsági fokozatától és attól függően, hogy a behatolás- és támadásjelző rendszer adott részegysége a felügyelt területen belül vagy kívül helyezkedik-e el." [10]

Szabotázsjelzés az érzékelendő szabotázsesemények függvényében a 3.- és 4. biztonsági fokozatban egyaránt az egyszerű eszközzel történő kinyitás, az I&HAS[2]komponensek felszerelési helyéről történő eltávolítása és érzékelő érzékelési irányának megváltoztatása esetében egyaránt kötelező elvárás. Szabotázsjelzés az akusztikus figyelmeztető eszközbe, valamint a CIE, ACE, SPT[3] eszközökbe történő behatolás esetén viszont csak a 4-es biztonsági fokozatban kötelező.

[2]I&HAS (intruder and hold-up alarm system) behatolás-és támadásjelző rendszer

[3]CIE (control and indicating equipment)vezérlő- és kijelző berendezés, ACE (ancillary control equipment)kiegészítő vezérlőberendezés, SPT (supervised premises transmitter)felügyelt létesítményiadó-vevő

A beléptetető rendszerrel szemben támasztott általános követelmények

Egy analitikai laboratórium beléptető rendszerének tervezésekor számos körülményt kell számításba venni, különösen a rendszerrel szemben támasztott követelményeinket illetően. Meg kell vizsgálni egyebek mellett az épület tereinek (zónáinak) sajátosságait, azokba a belépésre jogosultak körét, a veszélyes anyagok szempontjából ellenőrzött terek veszélyforrásait. Meg kell határozni, továbbá a beléptető rendszertől megkívánt funkciókat.

A laborépületbe történő be-, és kiléptetés a rendszer primer funkciója, valamint az objektumon belüli mozgások különböző jogosultsági szintek szerinti szabályozása. Napjainkban a jogosultság megállapíthatóságán kívül elvárható igény a jogosultság időben és térben történő lehatárolhatósága és változtathatósága. A beléptető rendszer személykövetési funkciója is lényeges, hiszen a belépésre jogosult tartózkodását, mozgását a laborban követni képes rendszer, nyílván tudja tartani, hogy az ellenőrzött terekben hányan tartózkodtak az időtartamokkal együtt. Az ideiglenes beléptetést megvalósító vendégkártya kezelési funkciója is lényeges a laborüzemeltetés szempontjából.

A laborüzemeltető szemszögéből elvárható igény a beléptető rendszerrel szemben az épület-felügyeleti funkció, amely lehetővé teszi a szellőztető rendszer ventillátorainak, a hűtőrendszer elemeinek a helységben tartózkodástól, illetve a bent-tartózkodók számától függő automatikus be-, és kikapcsolását. A korszerű szoftverek manapság lehetővé teszik, hogy meghatározott kimeneteket a beprogramozott bemeneti események bekövetkezéséhez hozzárendelve, feltételes műveleteket végezzen el a központ. Kamerákat kapcsolhat be pl. a méregraktár ajtajának, kinyitása, PLC-t (programozható logikai vezérlő) tartalmazó rendszer esetén a légtechnikai berendezés beindítható vagy leállítható különböző időszakokban, illetve eseményvezérelten.

Természetesen az események archiválása és tárolhatósága kiemelt jelentőségű funkciója a rendszernek, valamint a naplózás. Egy analitikai laboratórium esetében a fentieken kívül fontos követelmény a labort felügyelő veszélyes anyagok jelenlétét monitorozó alrendszer ellenőrzött terekben elhelyezett detektorainak beintegrálhatósága a komplex vagyonvédelmi rendszer elektronikai komponensébe.

Az analitikai laboratórium veszélyforrásait figyelembe véve a beléptető rendszernek képesnek kell lennie on-line üzemmódban működnie. Ez az üzemmód biztosítja számos, üzem-, és munkabiztonsági szempontból lényeges funkció installálását.

A beléptető rendszerek alapvető elemei, az objektumok, helyiségek, területek bejáratainál telepített belépési pontok az on-line rendszereknél helyi kommunikációs hálózaton keresztül számítógépes központhoz kapcsolódnak. [6] Ez a központ képes kell, hogy legyen több belépési pont üzemeltetése esetén is olyan bonyolult döntések meghozatalára, amely az adott ellenőrzött térben benntartózkodó személyek számának, jogosultságának, a laborban elvégzendő feladatok ellátásához kötött jogok meglétének (a meghatározott személyek előbbi szempont alapján történő minősítésnek), a védelmi monitorhálózat detektorai jelzésének, és egyéb, a létesítmény üzemelésének biztonságát biztosító technikai berendezés (pl. szellőztető motorok) működőképességéről jelentést adó szenzorok jelzéseinek együttes értékelését igényli. Ez elengedhetetlen, ha olyan biztonsági döntési mechanizmusok elvégzését kívánjuk meg, ami a laboratórium teljes biztonságtechnikai rendszerének állapotát figyelembe veszi. Amennyiben például a radiológiai laborban egyidejűleg munkát végző személyek megengedett száma a biztonságos munkavégzés feltételeként maximum 6 fő, akkor a hetedik belépését már nem engedélyezi a rendszer. Természetesen ilyen esetben több, más biztonsági elemmel szükséges megtámogatni a beléptető rendszert a kijátszhatóság minimalizálása céljából.

A beléptető rendszer on-line működését biztosító központ programja – amely egyébként a már meghatározott jogosultságok alapján a kontrollereket vezérli – esetünkben kell, hogy biztosítsa a következő lehetőségeket:

- Bizonyos terekbe csak kettesével biztosítson belépést, amennyiben a helyiség üres.
- Bizonyos helyzetekben oldjon az elektromotoros zár reteszelése
- Zóna-kiürülés esetén automatikus zárás
- Bent lévők listázása

Különös figyelmet kell fordítani az ellenőrzött területek behatolás-védelmére és beléptetés kontrolljára. A veszélyes anyagokat, az azokkal végzett tevékenységeket befogadó helyiségeket olyan beléptető rendszernek kell védenie, amely valamely fizikai eszköz (például proximity smart kártya) birtoklását és használatát követeli meg. Csupán egyfajta azonosítási elv alkalmazása azonban gyakran nem tekinthető kockázatarányos megoldásnak. Kiemelten védendő helyiségek esetében a biometrikus azonosítás, illetve a bizottsági típusú - legalább két személy együttes jelenlétét – megkövetelő megoldások alkalmazását is mérlegelni kell.

A beléptetésre ugyan alkalmasnak látszik valamely biometriai alapú személyazonosítással egybekötött beléptetés közvetlenül az érintett laborhelyiségekbe, ez azonban külön vizsgálatot igényel, hiszen a labormunka egyes sajátosságai kizárhatnak bizonyos eljárásokat. A vésznyitás lehetőségének biztosítása ugyanakkor minden rendszernél alapvető követelmény. A rendszer lehetővé kell, hogy tegye rendkívüli esemény bekövetkezésekor az áteresztési pontok azonnali nyitását, a bent tartózkodó személyek kimenekülése érdekében.

Az egyén ugyanis a bekövetkezett esemény másodlagos értékelése során, - amikor megállapítja, hogy a megküzdéshez elegendő-e az erőforrása, és a megoldási lehetősége – torzult értékelése miatt pánikba eshet, aminek kapcsán valósan romlik az esélye, hogy megtalálja a helyes megoldási módokat, és képes legyen részt venni a mentésben, önmentésben. [11]

A beléptető vezérlők tehát kell, hogy rendelkezzenek olyan bemenettel, amely a tűzjelző rendszer vagy a vésznyitó riasztását érzékelve automatikusan nyitják az áteresztő pontokat. Minden beléptetési ponthoz szükséges tervezni ajtónyitó eszközt (pánik gomb) veszélyhelyzet esetére. A vésznyitók általában beütő-gomb megoldásúak. Veszély (vagy annak érzete esetén) a gombát benyomva a kontroller az elektromos zár áramkörét megszakítva az ajtót nyithatóvá teszi. A vésznyitó gombok elsősorban a beléptető-terminálokkal védett belépési pontokkal határolt helyiségekbe kell, hogy felszerelésre kerüljenek, a laboratóriumba, az olvasók mellé. [5]

2. ábra. vésznyitó gomb
(forrás: Tunyogi-Berek)

Videó figyelő rendszer és „áruvédelem”

Munkaidő alatt a részleges élesítettségű státuszban lévő behatolásjelző rendszer védelmét a videó megfigyelő rendszer egészíti ki információ begyűjtésével, tárolásával. A videó megfigyelő rendszer a laboratóriumban lehetségesen előforduló számos esemény esetén hasznos segítséget jelenthet. A kameraállások kijelölésénél jó néhány kívánalomnak meg kell felelni. Egyrészt a kamerákat olyan pontokon kell elhelyezni, hogy az alkalmazási célnak megfelelő minőségben biztosítson értékelhető felvételt, méghozzá úgy, hogy csak biztonsági szempontból lényeges eseményről, illetve azonosítási cél esetén személyről készüljön felvétel. A kamerarendszer kiépítésénél tehát, mivel nem az elriasztás a fő cél a diszkrét elhelyezésre kell törekedni úgy, hogy a hatékonyság ne szenvedjen csorbát. A laborkomplexum irodahelyiségeit természetesen ide sorolva az öltöző, tisztálkodó, szociális helyiségek tereit nem kell kamerával megfigyelni. Ez egyrészt felesleges, másrészt zavarja a dolgozókat, azonban közlekedési útvonalaknál, a laboratóriumok egyes munkaterületein, (például a vegyi elszívófülkében) egy munkafolyamat rögzítése fontos dokumentum lehet baleset bekövetkeztekor. A méregraktár, az izotóptároló hasonló módon történő megfigyelése pedig betörés, vagy csempészés esetén jelentős segítséget nyújthat a tettes azonosításában.

A videó megfigyelő rendszer természetesen nem sértheti az ott dolgozó személyek alapvető jogait, nem szolgáltathat információt az irodákban folyó kutató és elemző tevékenységről. A térfelügyelet eme hatékony eleme kialakításánál fontos, hogy a rögzített kép az adatvédelmi jogszabályok figyelembevételével kerüljön rögzítésre és az elvárt képminőség, valamint a pontos időhöz történő időszinkronizálás biztosított legyen. Jelszavas beléptetés esetén lényeges elvárás, hogy a rendszer kameráit úgy kell elhelyezni, hogy az ne teremtsen lehetőséget a személyzet jelszavainak megfigyelésére, rögzítésére.

A laboratórium komplexumban felszerelt videó figyelő rendszerek több célt szolgálnak. Általánosságban elmondható, hogy vagyonvédelmi szempontból jelenlétük egyrészt visszatartó hatású a cselekménytől, másrészt a bekövetkezett esemény után az események könnyebben rekonstruálhatók. Biztonságtechnikai szempontból viszont lényeges a megfigyelt veszélyes munkaterekben végzett tevékenység során bekövetkezett nemkívánatos esemény utáni azonosítása a veszélyforrásnak, illetve a felelősség megállapítása. A célnak megfelelő kamera kiválasztását számos tényező befolyásolja. Meg kell vizsgálni azt, hogy az egyes kameráknak milyen környezetben kell működni, illetve milyen felbontású képet kell közvetíteni. Ez természetesen meghatározza az optika kiválasztását is.

A felbontást megvizsgálva általánosan elmondható, hogy a nagyfelbontású képet szolgáltató kamerák drágák, ezért a kamerákat feladat szerint optimalizálni kell. Gyakran a laboratóriumban rögzített képi információ későbbi elemzésére van szükség, melynek során folyamat felismerés, cselekmény, vagy személyazonosítás történik, így nagyfelbontású kamera alkalmazása ezeken a helyeken indokolt. Az érzékenységet tekintve a kamerákat beltéri körülmények között váltakozó fényviszonyok mellett kell működtetni, némelyiket a nap 24 órájában, ezért szükséges nagy érzékenységű kamerák alkalmazása.

Radioaktív készítményekkel végzett munkák alapvető követelményei tekintetében létesítményi sugárvédelmi szabályzat általában előírja, hogy „Radioaktív anyagok, illetve készítmények nyilvántartását úgy kell kialakítani, hogy az alapján az anyagok fajtája, mennyisége, holléte, rendeltetése, valamint folyamatban lévő felhasználása megállapítható és ellenőrizhető legyen.” Erre a célra távolról vezérelhető, a külső behatásoknak (vegyi, radiológiai) ellenálló, nagyfokú üzembiztonsággal működő, a kereskedelmi áruvédelmi rendszerek funkcióihoz hasonló feladatokat ellátó RF eszközökre lenne szükség. Amennyiben az igény a fenti megfogalmazott védelemre beigazolódik, szükséges vizsgálatokat követően

izotópok, vagy minták megjelölése után a rendszer azonnal képes lenne jelezni, ki,és mikor végzett műveletet valamely izotóppal, amennyiben a személyzet a mintatároló vagy az izotópszekrény és a minták/ izotópok is el vannak látva azonosító eszközökkel.

KÖVETKEZTETÉS

Egy olyan objektum kialakításakor és későbbi működtetésekor, melyben ideiglenesen vagy üzemszerűen tárolt anyagok jelenléte önmagában is veszélyforrást jelent, a veszélyes anyagok felügyeletének és ellenőrzésének javítása a meglévő nemzetközi kötelezettségeknek való megfelelés mellett és a felügyeleti és ellenőrző mechanizmusok alkalmazásának és technikai támogatottságának folyamatos vizsgálatát és tökéletesítését kívánja meg.

A laboratóriumokban és egyéb létesítményekben található fertőző és méreganyagokhoz való illetéktelen hozzáférésnek és azok eltulajdonításának megakadályozása érdekében azok védelmének biztosítása – ideértve a szállítást is kiemelt jelentőséggel bír. Ahhoz, hogy a védelem átfogó jellegű és állandón folyamatos maradjon a biztonságtechnikai alrendszerek felépítésénél a hatékonyságot fokozó komplexitás megvalósítása érdekében olyan feltételeket kell teremteni, melyek folyamatosan biztosítják az egyes alrendszerek és biztonsági modulok egymástól független működését is.

A behatolásjelző rendszer érzékelőiről és a speciális nukleáris, biológiai, és vegyi detektorokról, a meteorológiai érzékelőkről érkező jelzéseket olyan rendszernek kell feldolgoznia, amely alkalmas azok együttes kezelésére és vezérelni tudja a jelző-riasztó egységeket a szükséges épület-felügyeleti berendezésekkel együtt.

Vészhelyzetben a felügyeleti rendszer intézkedések sorozatát képes végrehajtani egyidejűleg, feladata alapvetően a vészhelyzetek megelőzése, így azok esetleges bekövetkezése esetén a létesítményi rendszer működésének élőerős támogatása szükséges. A felügyelt területek állapotát figyelve azonnal riasztania kell, annak érdekében, hogy a kezelő időben beavatkozhasson. A komplex védelem érzékeny pontját képezi a technológiai rendszer és a felügyelt terek állapotáról szóló információk, ezért a felügyeleti rendszernek biztosítania kell, hogy az információkhoz csak a jogosultak férhessenek hozzá. A létesítményben dolgozók feladata a riasztások kezelése és nyugtázása, ami felelősséget jelent. Ezért az épület-felügyeleti rendszerben a felelősségi szinteket és hatásköröket pontosan meg kell határozni.

A bűnös céllal felhasználni kívánt veszélyes anyagok, izotópok hozzáférési jogosultsággal rendelkező személyek által történő jogtalan eltulajdonítás tényét és módját a behatolásjelző rendszer sok esetben nem képes jelezni. A proxy kártya ellopható, a belépési azonosító kód eltulajdonítható, kizsarolható, stb. Ezekben az esetekben a beléptető-rendszerbe integrált videó megfigyelő rendszer szolgáltathat hasznos információt a belépő személy valódi azonosságáról.

A munkaidő alatti védelem másik hatásos eszköze a beléptető rendszer. Használatával regisztrálódik a belépni szándékozó kiléte, a belépés időpontja.

Az épületben meglévő vagyonvédelmi rendszerek – különös tekintettel a videó megfigyelő és a behatolásjelző rendszerekre – által szolgáltatott információ (videó képek, eseménylista, címkiosztás stb.) gondatlan kezelése nagymértékben növelheti az esetleges lopás (egyéb vétség, bűncselekmény) kockázati valószínűségét, és csökkentheti a komplex védelmi rendszer hatékonyságát. Ennek megfelelően az egyes központok eseménylistája, valamint a tárolt videó felvételek a laborkomplexum biztonságára nézve is érzékeny információkat rejthetnek, ezért az azokhoz történő hozzáférés jogosultságát szigorúan le kell szabályozni, illetve a hozzáférési jogosultsággal rendelkező személyek körét is minimálisra kell szabni.

Veszélyes anyagok vizsgálatát végző létesítmények védelmének kialakításakor a vagyonvédelmi koncepció helyes felépítésének köszönhetően a komplex biztonságtechnikai rendszernek képesnek kell lennie kezelni az épületfelügyeleti, a veszélyes anyagokat monitorozó eszközöket a vagyonvédelmi rendszer elemeivel együtt az operatív beavatkozás lehetőségeit biztosítva úgy, hogy a védelem elvárt szintjének fenntartása mellett a munkavégzés feltételei is teljesüljenek anélkül, hogy a létesítményben dolgozók fenyegetve éreznék magukat.

Felhasznált irodalom

[1] IAEA Illicit Trafficking Database *(ITDB)*, Office of Nuclear Security InternationalAtomic Energy Agency, 2009. http://www-ns.iaea.org/downloads/security/itdb-fact-sheet-2009.pdf

[2] Illicit Trafficking Database (ITDB) a Nemzetközi Atomenergia Ügynökség honlapján http://www-ns.iaea.org/security/itdb.asp, (letöltés: 2011. 05.26.)

[3] Berek Tamás: ABV (CBRN) analitikai laboratórium, mint művelettámogató speciális vegyivédelmi képesség, 2011. Hadmérnök, http://www.hadmernok.hu/2011_1_berek.pdf

[4] Berek Tamás - Pellérdi Rezső: ABV (CBRN) kihívásokra adott válaszlépések az EU-ban 2011. Bolyai Szemle XX. évf. 2. szám, ISSN: 1416-1443

[5] Berek Tamás: ABV (CBRN) analitikai laboratórium beléptető rendszere a biztonságos üzemeltetés szolgálatában 2011. Hadmérnök http://www.hadmernok.hu/2011_2_berek.pdf

[6] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Doktori (PhD) értekezés, 2009.

[7] Berek Tamás - Bodrácska Gyula: Az élőerős őrzés az objektumvédelem építőipari ágazatában, 2010. Hadmérnök, http://www.hadmernok.hu/2010_4_berek_bodracska.php

[8] Lázár Gábor - Szatmári-Juhász Ditta: A veszélyes anyagok közúti szállításának és tárolásának közbiztonsági aspektusai, 2011. Hadmérnök http://www.hadmernok.hu/2011_3_lazar_szatmari.php

[9] Móré Attila: MSZ EN 50131-1:2007/A1:2009. Riasztórendszerek. Behatolás- és támadásjelző rendszerek 1. rész: Rendszerkövetelmények in Detektor Plusz, 2010/ 1-2. sz.

[10] MSZ EN 50131-1:2011. Riasztórendszerek. Behatolás- és támadásjelző rendszerek

[11] Hornyacsek Júlia: A tömegkatasztrófák pszichés következményei, és az ellenük való védekezés lehetőségei, 2010. Bolyai Szemle XIX. évf. 4. szám, ISSN: 1416-1443

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Bunyitai Ákos
bunyitai.akos@gmail.com

A BELÉPTETŐ RENDSZEREK HELYE ÉS SZEREPE A VAGYONVÉDELEMBEN

Absztrakt

E rövid tudományos cikk célja a beléptető rendszerek vagyonvédelemben betöltött helyének és szerepének vizsgálata. Röviden összefoglalja az alapösszefüggéseket, definiálja a fogalmakat. Az elméleti tárgyaláson túl gyakorlati szempontból is megközelíti a tudományos problémát.

This short article is for investigate the access control system's functions in security. It gives a brief summary of the main definitions. Beyond the theoretical negotiation also includes practical support.

Kulcsszavak: *vagyonvédelem, beléptető rendszer ~ security, access control system*

BEVEZETÉS

A beléptető rendszerek elterjedtségéből adódóan szükségesnek véljük tudományos alapú vizsgálatukat, különös tekintettel a vagyonvédelemben betöltött helyükre, szerepükre, alkalmazási területükre vonatkozóan. A fentieken túl célszerűnek tartjuk a téma gyakorlatias megközelítését is, valamint a fejlődés irányának rövid bemutatását.

FOGALMAK, ALAPÖSSZEFÜGGÉSEK

Beléptető rendszer fogalma

„Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző pontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését.” „A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beléptetés felügyeletéhez szükségesek!”[1][2]

A beléptető rendszer fő részei [1]

- *Olvasó(k)* feladata, hogy az azonosításra alkalmas adatokat szolgáltassa a rendszer felé.
- *Vezérlő(k)* feladata, hogy az olvasóról beérkező adatok alapján eldöntse, hogy az adott személy az adott időpontban adott irányban jogosult-e az áthaladásra, működtesse, felügyelje az APAS-t (ld. később), naplózás.
- *Felügyeleti rendszer (pl.: PC-n futó felügyeleti szoftver):* feladata a rendszer ellenőrzése, a vezérlő egységek felprogramozása és a jogosultságok eldöntése, események rögzítése, visszakeresése, listázása.
- *Áthaladást szabályzó eszközök és érzékelőik* (a szakirodalomban az *APAS* rövidítés használatos az angol *Access Point Actuators and Sensors* meghatározásból) feladata, hogy kizárólag az arra jogosultak belépését tegye lehetővé (jogosulatlan személy be/ki lépésének akadályozása mechanikus vagy elektromechanikus eszközökkel), szingularizáció (egy azonosítás, egy áthaladás) és a gátló-szerkezet állapotának (nyitott, zárt, stb.) megállapítása. Pl.: forgókereszt, forgóvilla, gyorskapu, mágneszár, stb. érzékelőik működését a továbbiakban nem vizsgáljuk.

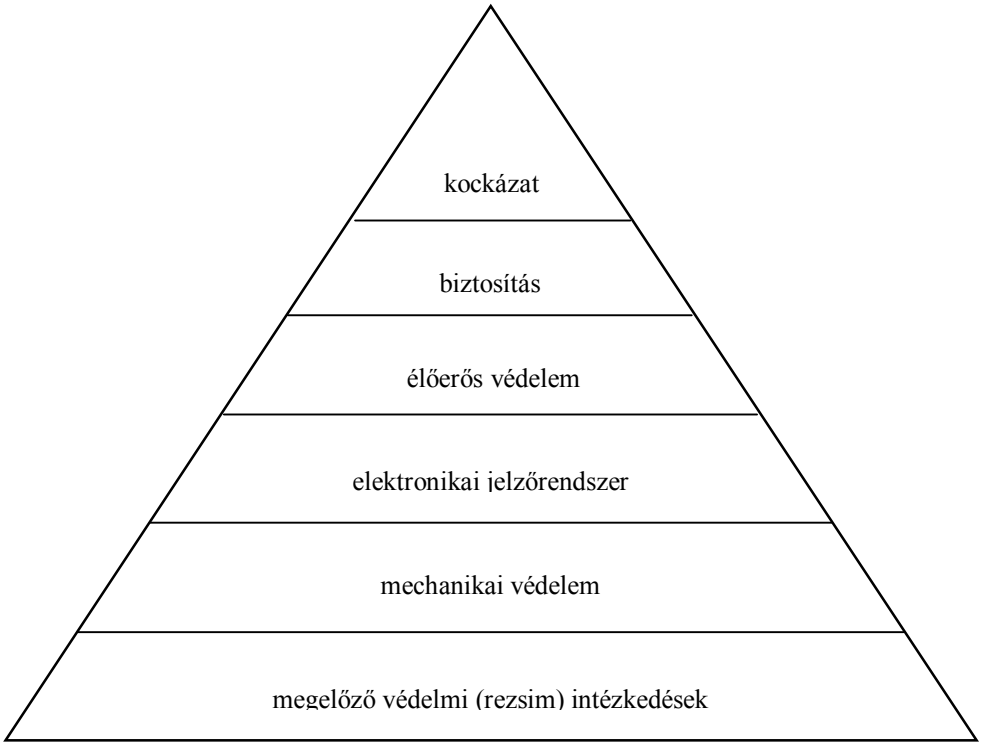
A *beléptetés folyamata:* azonosítás (személy, gépjármű, stb.), belépési jogosultság eldöntése, APAS működtetése, áthaladás, visszazárás. A beléptető további funkciói az események naplózása, rendszerfelügyelet, stb.[1]

A beléptető rendszer helye és szerepe a vagyonvédelemben

A beléptető rendszerek vagyonvédelemben betöltött szerepének vizsgálatához ismernünk kell a komplex vagyonvédelem megvalósításának elvi modelljét, vagyis a védelem megtervezésének lépcsőit és azok célszerűen alkalmazott arányait.

Az alábbiakban tekintsük a vagyonvédelem elvi felépítését ábrázoló vagyonvédelmi piramist!

A vagyonvédelmi piramis felépítése [3]:



1. ábra. A vagyonvédelmi piramis

- Megelező védelmi intézkedések célja olyan szabályok, szabályrendszerek bevezetése, betartása, betartatása, amelyek csökkentik a biztonsági kockázatot.
- Mechanikai védelem célja, hogy a védeni kívánt személytől, tárgytól, helyiségtől, információtól (információhordozótól) fizikailag távol tartsa a hozzáférési jogosultsággal nem rendelkező személyeket. Áthatolhatatlannak kell lennie a beavatkozó élőerő megérkezéséig.
- Elektronikai jelzőrendszer célja adott állapottól való eltérés (esemény) figyelése, rögzítése, továbbítása. Önmagában nem véd, csak jelez. Mind a mechanikai, mind az élőerős védelem támogatója lehet.
- Élőerős védelem célja, hogy nem kívánt folyamatokat megakadályozza. Az elsődleges beavatkozó megfelelő közelségben kell legyen, hogy időben történjen a beavatkozás.
- Biztosítás célja az eddigiekben tárgyalt eszközökkel gazdaságosan le nem fedhető kockázatok csökkentése.
- Kockázat azt jelenti, hogy mivel 100%-os biztonság nem létezik mindig számolni kell fennmaradó kockázattal.

A mai beléptető rendszerek a vagyonvédelem részét képzik, ellenőrzik, hogy a személy jogosult-e adott időpontban, adott irányban, adott átjárón való áthaladásra, vagyis a védett tértől távol tartható a belépésre jogosulatlan személy.

A beléptető rendszerek szűkebb értelemben az elektronikai jelzőrendszer részei. Tágabb értelemben azonban magukba foglalják (illetve szükséges kiegészítői): a rezsim intézkedéseket (pl.: kényszerített személyazonosítás), a mechanikai védelmet (pl.: forgóvilla) és az élőerős védelmet (pl.: vagyonőr, aki riasztás esetén beavatkozik) is. A fentiekből adódóan a beléptető rendszer egyéb rendszerekkel kiegészítve megvalósítja a komplex

vagyonvédelmet. Támogató rendszerekre az eltérő funkciókból adódóan van szükség. Hiszen a beléptető rendszer nem helyettesíti pl.: a kamerarendszert vagy a behatolásjelző rendszert.

Hol van szükség beléptető rendszerre? Hol, milyen rendszer javasolt?

Beléptető rendszerre szükség van minden olyan helyen, ahol a belépést felügyelni kell. Filkorn József – egy vezető beléptető rendszert fejlesztő, gyártó és forgalmazó cég műszaki igazgatója – szerint indokolt elektronikus beléptető rendszer létesítése, ha az alább felsorolt feltételekből bármelyik fennáll [4]:

- A védett terület biztonsága megköveteli
- Biztonságos (hamisíthatatlan) belépési kulcsra van szükség
- A belépőt azonosítani kell
- Tudni kell a védett területen tartózkodók számát
- Limitálni kell a védett területen tartózkodók számát
- Azonosítani kell a védett területen tartózkodókat
- Ki kell zárni a belépési jogosultság átruházásának lehetőségét
- Ki kell zárni, hogy jogosult beengedjen jogosulatlant
- Ki kell zárni a belépési kulcsok illetéktelenek általi felhasználását
- A belépést időben korlátozni kell
- Tudni kell, hogy az azonosított hol tartózkodik
- Tudni kell, hogy valaki mikor ment be, és mikor távozott
- Tudni kell, hogy egy adott területen ki, mennyi ideig tartózkodott
- Folyamatosan változik a belépésre jogosultak köre
- Egy átjáróhoz háromnál több kulcs kell
- Egy személynek háromnál több kulcsra van szüksége
- A belépésért díjat kell fizetni
- A védett területen való tartózkodásért (időarányos) díjat kell fizetni
- A védett területre való belépés különleges technológiai eljárást igényel

Jellemzően ilyen helyek az irodaházak, közép-és nagyvállalatok telephelyei, gyárak, uszodák, fürdők, szállodák, erőművek, katonai objektumok, stb.

A fentiekből következően valamely objektum beléptető rendszerének tervezésekor számos körülményt kell számításba venni, különösen a rendszerrel szemben támasztott követelményeinket illetően. Meg kell vizsgálni egyebek mellett az épület tereinek (zónáinak) sajátosságait, azokba a belépésre jogosultak körét, a bármely szempontból ellenőrzött terek veszélyforrásait. Bár a beléptető-rendszereknek a be-, és kiléptetés a primer funkciója, valamint az objektumon belüli mozgások különböző jogosultsági szintek szerinti szabályozása, napjainkban a jogosultság megállapíthatóságán kívül elvárható igény egyebek mellett a jogosultság időben és térben történő lehatárolhatósága és változtathatósága, így előre meg kell határozni a beléptető rendszertől megkívánt funkciókat.[5]

A téves következtetések elkerülése érdekében fontosnak tartjuk deklarálni az alábbiakat:

- Tökéletes, 100%-os biztonság nem létezik, minden rendszernek van gyenge pontja, minden rendszer kijátszható. A védelem szintje úgy értelmezhető, hogy milyen nehéz a komplex vagyonvédelmi rendszert megkerülni. Ennek megállapítására igen kevés objektív, mérésen alapuló eljárás ismeretes, a megfelelő rendszer tervezése mérnöki feladat. Köztudott, hogy egy lánc olyan erős, mint a leggyengébb láncszeme.
- A vagyonvédelem gyenge pontja nem csak a vagyonvédelmi piramis eleme lehet, hanem maga a felhasználó is. A mechanikai és elektronikai rendszerek szabotálása tervezhető. Az ember figyelmetlen, feledékeny, óvatlan, megzsarolható, megvesztegethető… vagyis megbízhatatlan. Vis maiorra nehéz tervezni.

- Mindhárom személyazonosítási módszernek (tudás, birtok, biometrikus tulajdonság alapú) vannak előnyei, hátrányai, javasolt és alkalmazott felhasználási területük eltér egymástól, ezért annak az esélye, hogy a közeljövőben valamelyik terület kiszorítja a másikat, minimális.
- Ma a tudás, a birtok és a biometria alapú beléptető rendszerek is kijátszhatók valamilyen módon. A tudás alapú az óvatlanságból, figyelmetlenségből, feledékenységből adódóan; a birtok alapú az átadhatóságból, másolhatóságból adódóan; a biometria alapú a minta másolhatóságából adódóan. A felhasználó kényszeríthető, hogy beüsse PIN kódját (erre az esetre használatos a duress, vagyis kényszerített kód), hogy átadja RF kártyáját vagy odatartsa ujját az olvasóhoz (ilyen esetre célszerű másik ujjat rögzíteni). Az előbbiek a mai közbiztonság mellett nem jellemzőek. Az ismert kijátszási módszerek ellehetetlenítésén fejlesztőmérnökök dolgoznak.
- A fentiekből nem következik, hogy egyik rendszer sem alkalmas feladatának ellátására. A biztonságtechnikai mérnök fő feladata az adott személy, tárgy, objektum, információ(hordozó) optimális védelmének tervezése. A kockázatok elemzése, a védett értéke, a lehetőségek, a kialakításra fordítható keretösszeg, a speciális igények figyelembevételével.
- A kockázatelemzést nem csak a rendszer tervezésekor, kivitelezésekor kell elvégezni, a körülmények üzemeltetés alatt is változhatnak!

Azokon a helyeken, ahol viszonylag nagyszámú felhasználót kell relatíve rövid idő alatt be-vagy kiléptetni, ott vonalkódos vagy rádió-frekvenciás azonosítás ajánlott. Vonalkódos azonosítás ott ajánlható, ahol a vagyonvédelem nem elsődleges (könnyedén reprodukálható), általában olcsón, nagy mennyiségű, egyszeri belépő kiadása indokolt (pl.: koncertjegy, parkolójegy, stb.). Kódos vagy biometrikus azonosítás nem ajánlott nagy forgalmú (nagy számú beléptetést igénylő) helyeken. Kódos azért nem, mert könnyen leleshető, elfelejthető. A kódok kiosztásánál ügyelni kell a kombinációk maximális számára és egyéb, a biztonságot befolyásoló tényezőkre (4 digites kód esetén maximum 10^4/2db kód osztható ki, ha van kényszerített kód, akkor maximum 10^4/4db, a kiosztásnál kerülni kell a 4 egyforma digitet „0000”, a számsorokat „1234” és két kód nem lehet egyforma). Biometrikus azért nem, mert kevésbé elfogadott és epidemiális kockázatok is jelentkezhetnek (kézgeometria azonosítás, tenyérerezet azonosítás, írisz-azonosítás, stb.). Ilyen, vagy kombinált személyazonosítású rendszerek kevesebb jogosult felhasználót érintő, fokozottabb biztonságot élvező helyiségbe jutáskor, a többkörös védelem részeként célszerű kialakítani, pl.: a vállalat szerverterme, TÜK-szoba, stb.

Mire jó még a beléptető rendszer?

A beléptető rendszerek – a fentieken túl – alkalmazhatók: jelenlét-figyelésre (ki, melyik helyiségben tartózkodik), munkaidő-nyilvántartásra, dolgozók adatainak nyilvántartására, programozott kimenetek vezérlésére, illetve integrált rendszer esetén minden gépészeti, tűz-és vagyonvédelmi feladat ellátására.

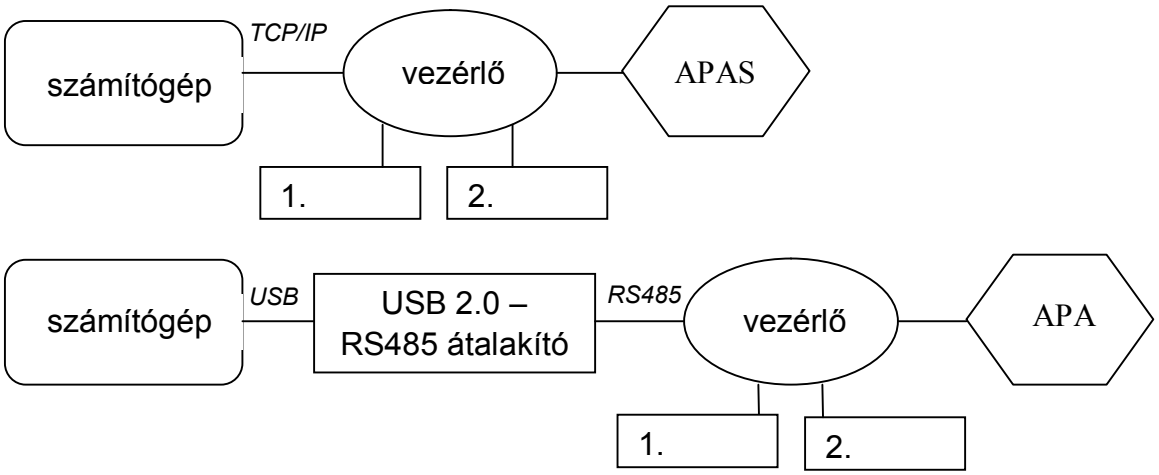
GYAKORLATI ISMERETEK

A beléptető rendszer felépítése, rendszertopológia

A továbbiakban tekintsük a fentiekben részletezett egységek egymáshoz kapcsolásának néhány lehetséges módját, vagyis hogyan lesz az alkatrészekből rendszer!

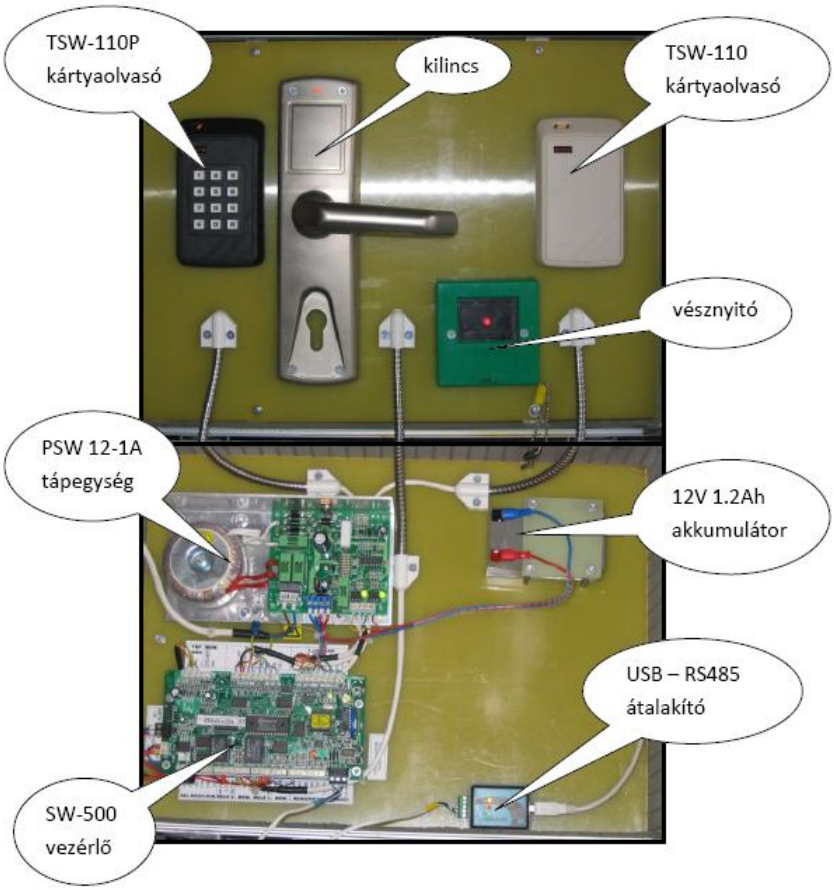
Az olvasó beolvassa az azonosításra alkalmas adatokat, majd ezeket továbbítja a vezérlő felé, ahol döntés születik az APAS vezérléséről. Mindenről esemény készül, ezt a vezérlő

tárolja és tovább is küldi a számítógép felé. Ld. 2/a. és 2/b. ábra, eltérés a vezérlő és a számítógép közti kommunikációs protokollban van. Ilyen rendszertopológia valósítható meg pl.: a Cryptex CR2001IP (2/a.ábra) és a Seawing SW-500 (2/b.ábra) vezérlőkkel.



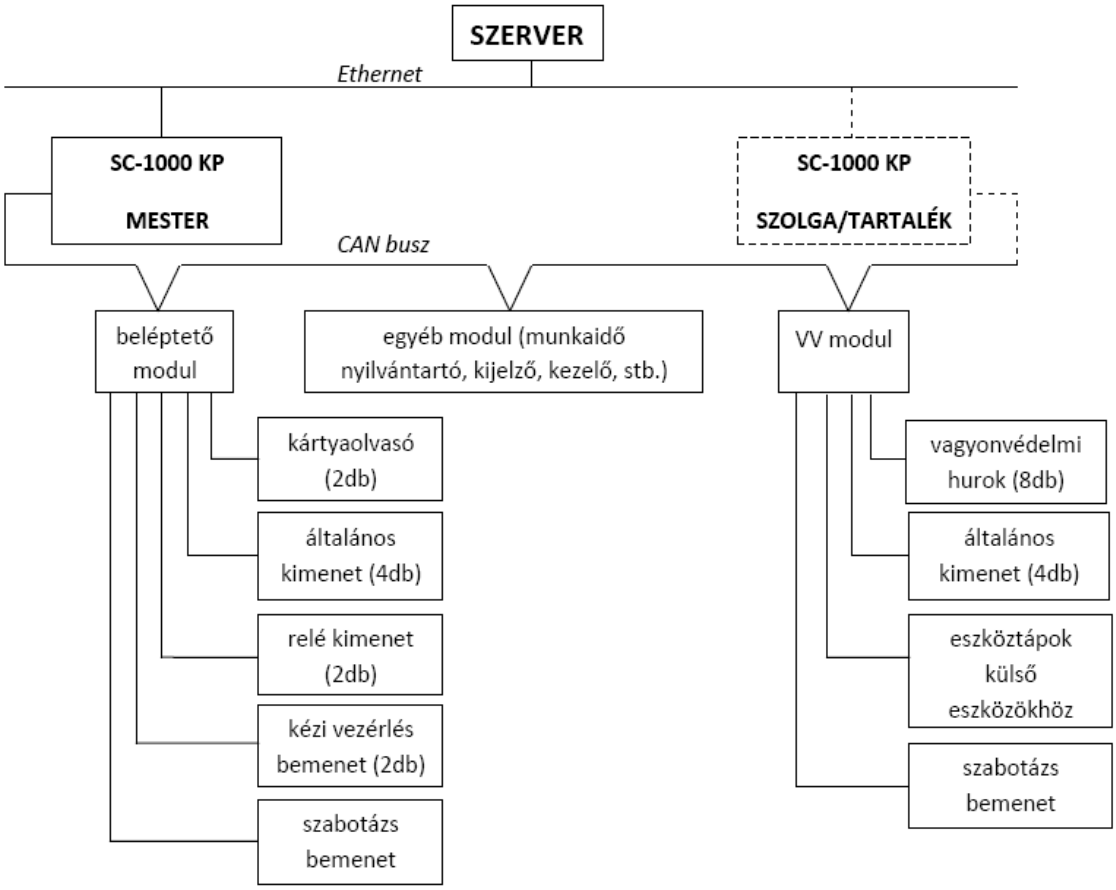
2/a-b ábra. Rendszertopológiai példák

Az alábbiakban – a könnyebb érthetőség kedvéért – a fenti (2/b.ábra) rendszertopológia megvalósítása kerül bemutatásra. Az alábbi ábrán (3. ábra) egy RFID beléptető rendszer látható, melynek elemei: SW-500 vezérlő, TSW-110 és TSW110P olvasók, PSW12-1A tápegység, akkumulátor, vésznyitó, elektronikusan reteszelhető kilincs, USB-RS485 átalakító. A tesztkészülékeket a kutatásokhoz a Seawing Kft. bocsátotta rendelkezésre.



3.ábra. A tesztbőrönd belseje

A továbbiakban röviden bemutatjuk a fejlesztések új irányának egyik képviselőjét, az SC-1000-res családot, mellyel integrált rendszer valósítható meg (4. ábra). A vezérlő CAN buszon kommunikál moduljaival, amelyeken keresztül csatolhatók a beléptető, vagyonvédelmi, munkaidő nyilvántartó, stb. eszközök, alrendszerek. A rendszertopológia és az eszközök nagy előnye az integrálhatóság, a széleskörű alkalmazhatóság, magas biztonsági szintű rendszer (Grade 4) valósítható meg velük, nagy kiterjedésű és/vagy több telephely integrált felügyelete lehetséges, RS485-höz képest gyorsabb adatforgalom. Az ikervezérlős kialakítás nagyobb megbízhatóságú rendszert eredményez, hiszen a vezérlő kiesésekor sem áll meg a rendszer, a felhasználókat nem érinti a jelenség.[6]



4. ábra. Az SC-1000 topológiája

Fontosnak tartjuk megjegyezni, hogy más gyártók szintén fejlesztenek hasonló termékeket, a fenti eszköz rövid leírásának célja nem a kiemelés, hanem a fejlesztés irányának bemutatása.

Mire kell ügyelni beléptető rendszer tervezésekor, kivitelezésekor?

- A tervezés első szakasza a kockázatelemzés és igényfelmérés
  - mit kell védeni
  - mitől kell védeni
  - mekkora a rendelkezésre álló keretösszeg
  - milyen speciális igények vannak
- A fentiekből el kell dönteni, hogy milyen védelmi szintű rendszer kerüljön kialakításra és milyen eszközökkel.
- Ügyelni kell a megkerülhetetlenségre és kijátszhatatlanságra
  - megkerülhetetlenség: a védendő tér összes belépési pontját védjük

    - kijátszhatatlanság: szingularizáció, megfelelő nyitvatartási idők és anti-passback beállítások
- Életvédelmi előírások betartása
    - menekülési útvonalak szabaddá tétele (vésznyitó vagy pánikkar felszerelése)
    - az áthaladást szabályzó eszközök átbocsátó képességének figyelembe vétele
    - zsilipben nem ragadhat benn senki
- Empátia
    - feleslegesen ne akadályozza a rendszer a védett objektum használóinak szabad mozgását
    - karbantartó, postás, szállító, vendég, stb. bejutását (kijutását) is meg kell oldani (jellemzően a recepcióhoz) pl.: kaputelefon és távnyitó alkalmazásával
- Dokumentáció a kivitelezéshez
- Telepítéskor
    - vezérlő csak a védett térrészben lehet
    - kábelezés csak a védett térben lehet, vagy ugyan olyan szintű védelemmel kell ellátni, mintha ott lenne, olvasók megfelelő magasságba telepítése, átolvasás tervezése
- Megvalósulási dokumentáció a karbantartáshoz, szervízeléshez

A (NEM TÚL TÁVOLI) JÖVŐ

A fejlődés iránya a különböző rendszerek integrálása felé vezet. Ma is számtalan termék létezik, mely egyszerre, integráltan képes kezelni az épületfelügyeleti (világítás, fűtés, melegvíz, árnyékolás, légkondicionáló, stb.), tűz (tűzjelző és tűzoltó) és vagyonvédelmi (behatolásjelző, beléptető, kamera, stb.) rendszert, egységes felületen megjelenítve. Ahhoz viszont, hogy ez a rendszerstruktúra széles körben megjelenjen és elterjedjen, mindenki számára elérhetővé váljon, el kell telnie néhány évnek. A későbbiekben elképzelhető, hogy minden épületben az ott lévő összes elektromos berendezés informatikai kapcsolatban lesz egymással. Ennek előnye lenne, hogy kényelmes, egy felületen könnyen és átláthatóan kezelhetővé válna minden, gazdaságos (pl. lekapcsolódik a villany, ha nem tartózkodik senki a helyiségben), illetve kitágulna az egyes eszközök funkciója (pl. a TV segítségével videó-telefonálhatnánk, a kamerarendszer segítségével videó-üzeneteket küldhetnénk) stb. Hátránya az elektromos áramtól való nagyobb mértékű függés.

Tekintsük példaként az alábbi szituációt: behatolás történik egy családi házba vagy lakásba éjszaka, amikor a tulajdonos otthon van. A rendszer értesíti a rendőrséget a kamerarendszer első képeivel és a GPS pozíció megjelölésével. Lezárja a helyiséget, amelyben a behatoló tartózkodik („nem büntethető, akinek a cselekménye a saját, illetőleg a mások személye, javai vagy közérdek ellen intézett, illetőleg ezeket közvetlenül fenyegető jogtalan támadás elhárításához szükséges” [7]) – vagy ahol a tulajdonos tartózkodik – a tulajdonos és családja, anyagi javai védelme és a hatóság munkájának segítése érdekében, blokkolja a helyiségben található összes konnektort.

Egy másik példa: tűz üt ki, a jelző-és oltórendszer aktivizálódik, értesíti a tűzoltóságot és felhívja a figyelmet az épületben tartózkodó személyekre. Megkezdődik a kiürítés, biztosítja a megfelelő tájékoztatást, a kiürítési utak nyílászáróit oldja, akár intelligensen a tüzet elkerülve vezeti a bent lévőket. A felvonókat az alsó szintre irányítja, esetleg plusz információkkal látja el a tűzoltóságot (elküldi az épület alaprajzát, a tűz lokalizálása, gócpontja, mi ég, milyen anyagok találhatók a közelben és milyen mennyiségben, mekkora a helyiség belső hőmérséklete és milyen gázok találhatók a légterében stb.). Lekapcsolnak a közművek, a tűzoltóság megérkezéséig kinyílnak a kapuk és ajtók a könnyebb megközelítés érdekében,

részükre megfelelő kommunikációs hálózatot biztosít. Értesíti a tulajdonost, a tűz lefeketítése után szellőztetés indul, a rendszer ön-kárfelmérést végez.

Feltételezzük hogy a fentiekhez hasonló rendszer hasznára válna a társadalomnak.

ÖSSZEGZÉS

A fentiekből látható – az alapfogalmakon és összefüggéseken túl – hogy mire alkalmas egy beléptető rendszer, hol milyen rendszer javasolt. Röviden bemutattuk a beléptető rendszerek felépítését, konkrét, széles körben alkalmazott eszközök rövid bemutatásán keresztül rendszertopológiai példákat hoztunk. Elképzeltünk egy mindenki számára elérhető integrált rendszert, mely segít az épületfelügyeleti, tűz és vagyonvédelmi rendszereket felügyelni, átlátni.

Felhasznált irodalom

[1] Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból, Hadmérnök, VI. Évfolyam 1. szám, 2011/1, ISSN1788-1919, http://hadmernok.hu/2011_1_bunyitai.pdf

[2] Filkorn József: Beléptető rendszerek c. előadás, Seawing Kft, Székesfehérvár, 2009.

[3] Dr. Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései c. PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009.

[4] Interjú Filkorn Józseffel, Székesfehérvár, 2011.

[5] Dr. Berek Tamás: ABV (CBRN) analitikai laboratórium beléptetőrendszere a biztonságos üzemeltetés szolgálatában, Hadmérnök, VI. Évfolyam 2. szám, 2011/2, ISSN1788-1919, http://www.hadmernok.hu/2011_2_berek.pdf

[6] Seawing SC-1000 műszaki paraméterek, 2010.

[7] 1978. évi IV. törvény a Büntető Törvénykönyvről, A jogos védelem 29.§ 1)

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Lasz György
georgelasz@gmail.com

A SZEMÉLYBIZTOSÍTÁS SPECIFIKUMAI A MAGÁNBIZTONSÁGI SZOLGÁLTATÓ ESETÉN

Absztrakt

Életet adni az életért - a legnagyobb vállalás. Ez már nem üzleti elkötelezettség, hanem a hivatás mélyről fakadó, meggyőző szeretete. Nemcsak a magán biztonsági szolgálatoknak delegált feladatok, de ezek szabályozása is eltérő a tagállamokban. Időrendi sorrendben a magán biztonsági szolgálatokra vonatkozó törvényi szabályozás az 1990-es évek elején jelent meg Nyugat-Európában, és az 1990-es évek végén, a XXI sz. elején jelent meg Kelet-Európában. Két kivétel van: Olaszország 1931-es törvényével, és Svédország, ahol 1974-ben született meg a jogszabály. A kötelező képzés megszervezése sem egységes az Unión belül; van ahol ez állami feladat, van ahol magán. Spanyolországban a képzés megszervezése, a tanárok akkreditálása és a majdnem 500 képzési centrum engedélyezése a rendőrség felügyelete alá tartozik. A rendőrség tartja a magáncégekhez jelentkezők felvételi vizsgáját is. A normák és a Közösségi gyakorlat áttekintését követően cikkemben a cégünk által formált személyvédelmi gyakorlatról szólok.

Giving life to life - the biggest assumption. This is not a business commitment yet, but the deep, convincing affection for profession. Not only the tasks belong to the private security services, but regulation of these as well are different in the Member States. In chronological order the legal regulation of private security services appeared in Western Europe in the early 1990's, and in Eastern Europe in the end of the 1990's, in the early 21st century. There are two exceptions: Italy with its act of 1931, and Sweden where the law was made in 1974. Also the organisation of compulsory training is not unitary in Union; somewhere this is a duty of state, somewhere this is private. In Spain the organisation of training, accreditation of teachers, and authorization of the almost 500 training centre are under the police surveillance. The police holds also the entrance exam for those who applied to private businesses. After reviewing the norms and the Community practice my article will discuss the close protection practice formed by our business.

Kulcsszavak: *magánbiztonság, személyvédelem, képzés ~ private safety, close protection, training*

A MAGÁNBIZTONSÁGBAN DOLGOZÓK KÉPZÉSE EURÓPÁBAN

Be kell látnunk, hogy a magán biztonsági szolgáltatók egyre nagyobb szerepet játszanak az állampolgárok biztonságának megteremtésében. Az állami rendészet energiái végesek, azok a közterületen megvalósuló cselekményekre és bűncselekményekre fókuszálódnak elsődlegesen. A magánbiztonsági szektorral történő kooperáció egyet jelent a felelősségvállalással, a hatékonyság növelésével, és a biztonsági igények megfelelő kielégítésével, speciális helyzetek rugalmasabb és sokszor olcsóbb megoldásával s nem utolsó sorban a magasabb fokú biztonság megteremtésének igényével. Az állam mindenkori feladata a biztonsági szektor hatályos jogszabályoknak megfelelő felügyelete, a jogi normakörnyezet igényekhez történő igazítása. Franciaország, és megannyi európai ország, úgy döntött szigorúbban ellenőrzi a magán biztonsági szektorban tevékenykedő cégeket. A szektor most már csak a megelőzésért felel, és a képzést, valamint a szakmai etikát szigorú irányelvek vezetik.1

Vallom, kutatásaim s tapasztalataim okán, hogy az állami szerveknek jobban meg kell ismerniük a magán biztonsági szektort, annak érdekében, hogy korrekt verseny, valamint együttműködés alakulhasson ki köztük. A magánbiztonsági cégek megbízhatóságát, szolgáltatásuk színvonalának jelentős növekedését és kiszámíthatóbbá válását nem kicsiny részben a képzés, a rendszeres képzés teremtheti meg. Az állampolgárok érdekeit tartja szem előtt a CoESS általam később bemutatott elemzése is, amely vizsgálja a magánbiztonsági szektor több vertikumát, azonban itt most leginkább a jogszabályi hátterére, a képzés jelentőségére és az Unión belüli különbözőségekre és azonosságokra koncentrálok.

Nemcsak a magán biztonsági szolgálatoknak delegált feladatok, de ezek szabályozása is eltérő a tagállamokban. Időrendi sorrendben a magánbiztonsági szolgálatokra vonatkozó törvényi szabályozás az 1990-es évek elején jelent meg Nyugat Európában, és az 1990-es évek végén, illetve még később jelent meg Kelet-Európában. Két kivétel itt is akad: Olaszország 1931-ben alkotott, valamint Svédország, 1974-ben született meg a szabályozásával.[2]

Ha a tagállamokat rangsorolnánk a szabályozások "szigorúsága" szerint, Spanyolország állna az első helyen. A szabályozást[3] néhány cég túl szigorúnak tartja, amit az EU is elismer. Az EU a törvényt ellentétesnek találta az Unió szabad mozgásról szóló alapelvével és kérésére a törvényt azóta módosították.[4] A spanyol szabályozás az egyik legrészletesebb: követelményeket állit az egyenruha, a fegyverek, a gépjárműpark, az őrkutyák, de még a cégek pénzügyi mutatóira vonatkozóan is. A törvény a magán biztonsági szolgálatok által végrehajtható feladatokat is megnevezi. A magán biztonsági szolgálatok saját védelmüket nem láthatják el, egy erre szakosodott szolgáltatóval kell szerződniük. A spanyol törvény a belga törvényt[5] vette modellül. A törvény megnevezi a magán biztonsági szolgálatok által végrehajtható feladatokat és követelményeket állit az egyenruha, a fegyverek, a gépjárműpark

[1] Így vélekedik Michélet Alliot-Marie, a francia belügy és tengerentúli területek minisztere. Innen: COESS, (2008): La participation de la sécurité privée á la sécurité génerale en Europe. CoESS – Confederation of European Security Services.Livre Blanc, Décembre 2008. Institut National des Hautes Etudes de Securite, France."Vhite paper Private Security". A dokumentumot francia nyelven dr. Finszter Géza, az Országos Kriminológiai Intézet munkatársa bocsátotta rendelkezésünkre, elérhető az In-Kal Security 2000 Kft. archívumában.

[2] U.o.

[3] Az 1992. július 30-án elfogadott törvényt módosították, 1999 január 29-én Királyi rendeletben és a 2007 szeptember14-ei Királyi Rendeletben.

[4] Az Európai Bíróság a törvényt 1998-ban ellentétesnek találta az EU alapelveivel, mert biztonsági őrök kizárólag spanyol állampolgárok lehettek, majd 2002-ben mert a külföldön bejegyzett cégeket hátrányosan megkülönböztette.

[5] A magánbiztonsági szolgálatokról és a speciális biztonságról szóló 1990-ben elfogadott norma

és az őrképzés vonatkozásában. A spanyol törvény alapján született meg a portugál törvény 2004-ben. Spanyolországnak, Belgiumnak és Portugáliának van a legszigorúbb törvénye a magán biztonsági szolgálatokat illetően.

Svédországban a szakmai szabályrendszer többszintű: a törvény irányelveket, elvárásokat fogalmaz meg a szakmának[6], a kormányzati határozatok az irányelvek végrehajtását szabják meg, míg az országos rendőrkapitányság az ehhez tartozó követelményeket, standardokat állítja fel. A törvény követelményeket állit az egyenruha, a fegyverek, a gépjárműpark és az őrképzés vonatkozásában. Ez a szabályozás rendkívül érdekes. A társadalmi párbeszédről híres Svédország jelen törvénye is a magánszférával történt egyeztetés után született meg. A cégek pedig alkalmazottaik álláspontját képviselték. Ezért a törvényi szabályozásokat a szakma eelfogadta. A volt Keleti blokk tagországai is a szigorú szabályozással rendelkező országok csoportjához sorolhatók. Szlovákiában a Belügyminisztériumhoz tartozó magánbiztonsági hivatal négy területen tevékenykedik:

- törvényi változást sürget;
- meghatározza a metodikát;
- megszervezi a szakvizsgákat;
- felügyeli a cégek tevékenységét.

Északi szomszédunknál, Szlovákiában[7] a magán biztonsági szolgálatok állami felügyelet alatt állnak. Romániában[8] és hazánkban[9] ehhez hasonló a törvényi szabályozás. Majdnem minden vizsgált tagországban a biztonsági őrök valamiféle szakmai képzést kapnak. Kivétel Németország, ahol a jelentkezők vagy az Ipari és Kereskedelmi Kamara által szervezett szóbeli vizsgán vesznek részt, vagy 40 órás képzésen, amely azonban nem állit vizsgakövetelményt. A többi tagországban a képzés időtartama nagyon különböző. A leghosszabb képzés Magyarországon van 320-430 óra, a választott szolgálati területtől függően (biztonsági felügyelet, pénzszállítás, személyvédelem). Svédországban a követelmény 40 óra, Spanyolországban 180 óra, Lettországban 160 óra. Romániában a választott szolgálati területtől függően 90-360 óra a képzés tartama. A többi tagországban a következőképpen oszlik meg a képzés: Portugália 130 óra, Denmark 111 óra, Finnország 100 óra, Szlovákia 70-90 óra a választott szolgálati területtől függően, Franciaország 70 óra, Belgium 66 óra a beosztottaknak és 72 óra a vezetőknek. Az Egyesült Királyságban 32 óra képzést írnak elő. A továbbképzés kérdése is különbözően szabályozott a tagországokban. Spanyolországban kötelező a 20 órás éves továbbképzés, míg Svédországban háromévenként egy hét továbbképzés a követelmény, végül Belgiumban 32 óra ötévenként.

A kötelező képzés megszervezése sem egységes az Unión belül; van ahol ez állami feladat, van ahol magán. Spanyolországban a képzés megszervezése, a tanárok akkreditálása és a majdnem 500 különféle képzési centrum (tornatermektől a taktikai helyiségekig) engedélyezése az állami rendőrség felügyelete alá tartozik. A rendőrség tartja a magáncégekhez jelentkezők felvételi vizsgáját is.[10] Ezzel a gyakorlattal magam is azonosulok. A fegyvertartási engedélyek kiadása és a kiképzés a Guardia civil hatáskörébe tartozik. Romániában is állami feladat a biztonsági őr képzés megszervezése. A rendőrség kidolgozza a tananyagot, majd engedélyezteti a Kormányfővel, a Belügyminisztériummal és az Oktatási Minisztériummal. A vizsgabizottságok legalább egy tagja rendőrtiszt! A képzést sokszor aránytalanul nehéznek tartják a tényleges feladatellátás szempontjából. Sokan kifogásolják,

[6] A magán biztonsági szektor törvénye 1974
[7] A Szlovák Nemzeti Tanács 379/1997 határozata alapján
[8] 333/2003 Törvény a területek, személyek és áruk biztonságáról és őrzéséről.
[9] 2005. évi CXXXIII. Törvény
[10] 68 alkalommal 1997 óta

hogy a külalakot többre értékelik az ügyfelekkel tanúsított magatartásnál.[11] A jövőben érdekes kutatásnak tartanék egy, a biztonsági őrök képzését, továbbképzését reprezentáló kutatást, amely interjúkkal a vizsgára is koncentrál.

Szlovákiában az állam nem vesz részt az oktatásban, a képzést magáncégek végzik. A tanárokkal szembeni követelmény legalább 5 éves biztonsági szolgálati jogviszony és a Belügyminisztérium által kiadott engedély, amely 10 évig érvényes. A tananyag tartalma és a tanuló- tanár arányszámot is felügyeli a belügyi tárca.[12] Magyarországon a rendőrség közreműködött a tananyag elkészítésében. Az Egyesült Királyságban csak az érzékeny területeken dolgozó biztonsági őrök kapnak rendőrség által kialakított képzést. Franciaországban és Belgiumban a belső vagy külső szolgáltató képzési centrumait a Belügyminisztérium engedélyezi. Svédországban professzionális magán Képzési Központok vannak, amelyeket a helyi hatóságok engedélyeznek. Több mint egy tucat ilyen képzési központ van, és a nyújtott képzés minőségét a hatóság monitorozza. A képzés minősége nemzetközileg elismert és elfogadott. A rendőrség az önvédelmet oktató tanárokat képzi.

Végül Németországban a képzést az Ipari és Kereskedelmi Kamara és szakmai szervezetek tartják, míg a tananyagot a tartományok dolgozzák ki. A képzést biztosító szervezeteknek nem kell külön engedély, valamint az álláskeresők átképzését a tartományi kormányok finanszírozzák.

Mindez azonban csak a biztonsági őr képzésre vonatkozó szabályozás, meg kell vallani, a személyvédelem specifikumait intézményi rendszerben nem tanulhatják a leendő testőrök. A következő részben azt mutatom be, mi hogyan tanítjuk és tesszük e tevékenységet.

AZ ÁLTALUNK MEGVALÓSÍTOTT SZEMÉLYVÉDELEM[13]

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályáról szóló 2005. évi CXXXIII. törvény 74.§ 1. pont d.) alpontja alapján a természetes személyek életének és testi épségének védelme az egyik szolgáltatási fajta, amelyet más jogszabály testőri szolgáltatásnak is nevez, az ahhoz szükséges rész-szakképesítést pedig testőri szakképesítésnek. Mások személyvédelemnek nevezik ezt a szolgáltatási fajtát.

A személyvédelem, megítélésünk szerint a következő formában hajtható végre:

- közvetlen személyőrzés;
- lakóhely, ideiglenes szálláshely biztosítás;
- munkahely biztosítás;
- rendezvény- és programhely biztosítás;
- biztosítás a közlekedésben.

A személyvédelem a védett személy biztosítása a személyvédelmi formákban.

A személyvédelem végrehajtásának mozzanatai, színterei:

- A védett személy tanulmányozása, védelmi igényeinek megismerése, személyes beszélgetés, információgyűjtés módszerével.
- A védett személy életét, testi épségét, egészségét veszélyeztető források, kockázati tényezők felmérése, értékelése.
- A személyvédelmi terv kidolgozása.

[11] Sok panasz van a biztonsági őrök fizikai erővel való visszaéléssel kapcsolatosan.
[12] Max 30 fős csoportokban van erre lehetőség
[13] BÖKÖNYI István - JÁRMY Tibor: A magánbiztonság főszereplője: a biztonsági őr. Jegyzet az In-Kal Security 2000 Kft. Biztonsági őr (Vagyonőr, Testőr) szakképzésének hallgatói számára. Budapest, 2009. ISBN: 978-963-06-7951-0

- A személyvédelem tervet végrehajtó állomány felkészítése a terv végrehajtására.
- A közvetlen személyőrzés végrehajtása testőrrel (testőrökkel).
- A védett személy lakóhelye, szálláshelye biztosításának végrehajtása.
- - A védett személy munkahelye biztosításának végrehajtása.
- - A védett személy biztosításának végrehajtása rendezvényeket, rendezvénynek nem minősülő más programokon.
- - A védett személy biztosítása gépkocsival történő közlekedés esetén, tömegközlekedési eszközön, vasúton, hajón, repülőgépen.

A biztonsági őrök, mint testőrök legtöbbször közvetlen személyőrzési feladatokat látnak el. A közvetlen személyőrzés végrehajtható gyalogosan egy fős, két fős, három fős, négy fős, öt fős, hat fős gyalogos védelmi alakzatban. Az ilyen alakzatokat a háromtól hatfős alakzatokig egy védelmi gyűrűbe szervezzük. Tömegben, fokozott kockázat, és veszélyhelyzet esetén legalább kilenc fő testőr részvételével, két védelmi gyűrű, legalább 15 fő testőr alkalmazásával három gyalogos védelmi gyűrű is kialakítható a védett személy körül.

A közvetlen személyőrzés gyalogos alakzatainak kialakítását, az alakzatok mozgását a gyakorlati foglalkozásokon sajátítják el a testőr rész-szakképesítési oktatásban résztvevők.

1. ábra. Személybiztosítási alakzat 1 fős

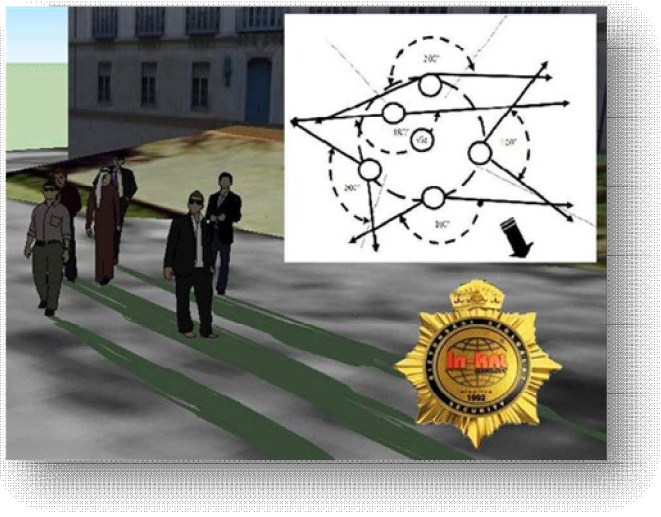
A közvetlen személyőrzés végrehajtása napjainkban leggyakrabban személygépkocsival történik. A védett személy gépkocsiját állandóan őrzött parkolóban, vagy zárt garázsban kell tartani. Elindulás előtt minden esetben át kell vizsgálni a gépkocsit, ide értve a motorházat, utasteret, csomagteret, az alvázat, a kerekeket, a gépkocsiban lévő audio-vizuális szórakoztató eszközöket. A gépkocsiban legyen tűzoltó készülék, ablaktörő kalapács, az életmentéshez, elsősegélynyújtáshoz szükséges egészségügyi csomag, lövedékálló mellény, 2 db pótkerék.

Amennyiben a védett személyt szállító gépkocsi vezetője egyben testőr is, a védett személy a hátsó ülésen, mögötte üljön. Amennyiben egy testőr is tartózkodik az autóban a gépkocsivezetőn kívül, a testőr a jobb első ülésen üljön, a védett személy pedig a testőr mögött foglal helyet. Amennyiben a gépkocsiban egy gépkocsivezető és két testőr is tartózkodik, az egyik testőr a jobb első ülésen, a másik testőr a gépkocsivezető mögött üljön, a védett személy pedig a jobb első ülésen ülő testőr mögött foglaljon helyet.

2. ábra. Személybiztosítás 3 fős alakzatban

Több gépkocsival történő közvetlen személyőrzés esetén a védett személy az első gépkocsiban utazzon egy gépkocsivezetővel és egy vagy két testőrrel. A második – követő – gépkocsiban utazzon olyan testőrcsoport, amely felveszi a harcot az esetleges támadó személyekkel, és fedezi az első gépkocsi menekülését, amely a védett személy kivonását, menekülését végzi a veszélyes helyszínről.

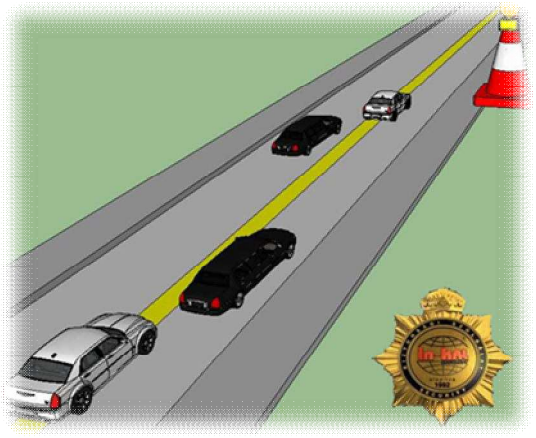
A lakóhely, ideiglenes szálláshely biztosítása történhet soklakásos blokkházban, többlakásos társasházban, családi házban, villalakásban. A biztosítás történhet a lakóhelyen kívüli figyelő eszközökkel, álló vagy mozgó biztosító őrökkel, biztosító járőrökkel. Minden esetben tervezni kell több menekülési útvonalat rendkívüli események bekövetkezésének esetére. A munkahely biztosítása függ a munkahely elhelyezési körülményeitől, a munkatársak számától, a munkahelyre a külső, ismeretlen személyek belépési lehetőségeitől, a munkahelyet védő biztonságtechnikai rendszer kiépítettségétől. Célszerű, ha a munkahelyet biztosító testőröket, munkatársaknak álcázzák a biztosítást szervező, vezető személyek. A munkahely biztosításával is tervezni kell a menekülési útvonalakat.



3. ábra. Védelmi alakzat

A rendezvényeken való megjelenés esetén szükséges a rendezvényhelyszín előzetes átvizsgálása, a védett személy rendezvényen történő közvetlen személyőrzése gyalogos alakzatokban, továbbá a menekítési útvonalak tervezése is.

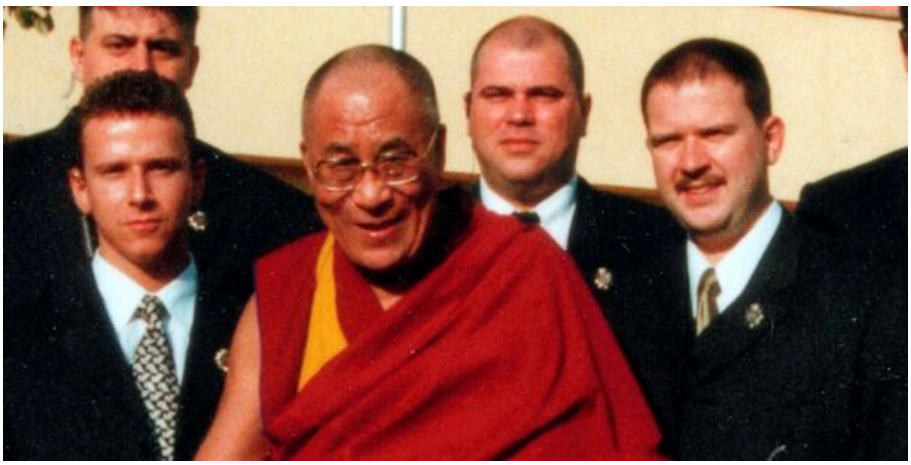
A biztosítás a közlekedésben megvalósulhat gépkocsiban biztosítással. A védett személy közforgalmi tömegközlekedési eszközökön utazásánál mindig a testőrnek (testőröknek) kell előbb felszállnia a járműre, illetve neki (nekik) kell elsőként leszállnia, a védett személy a testőr (testőrök) után szálljon fel, illetve szálljon le. A testőr a védett személy mellett álljon, vagy üljön a tömegközlekedési eszközön. Több testőr védelmi gyűrűt is alkothat a védett személy körül a tömegközlekedési eszközön. Vasúton történő utazásnál előzetesen a felszálló testőr vizsgálja át a vasúti kocsit, ideértve a mosdót is. Hajón történő utazásnál a testőrök gondoskodjanak külön mentőmellényről a védett személy számára.



4. ábra. Biztosítás gépjárművel

A LEGSZEMÉLYESEBB KAPCSOLAT

Nagyon büszkék vagyunk arra, hogy az általunk védett személyek biztosításakor teljesítményünk minden esetben a legnagyobb elismerést vívta ki nem csak a védett személy, (sok esetben annak kormánya, saját biztosító csapata), hanem a szűkebb és tágabb szakma előtt is.



1. kép. Sokak mellett a Dalai Láma biztonságát is szavatoltuk Magyarországon

Ennek megfelelni, erre a minőségre hosszú távon garanciát vállalni, a legszilárdabb szakmai meggyőződésem szerint csak akkor lehet, ha a nemzetközi tapasztalatok birtokában, a legkorszerűbb technikai környezetben, folyamatos és állandó képzésben tartjuk a személybiztosításban részt vevő testőreinket. E hivatás nem örök életre szól. A fokozott pszichikai terhelés, sok esetben a biztonságot jelentő család hiánya, a napi legalább 12 órás folyamatos szolgálat, a fizikai, erőnléti vizsgák csak a legelhivatottabbaknak, és karrierjük csúcsán biztosítja ezen örök életre szóló, egyedüli munkát. "A legszemélyesebb kapcsolat" ez,

amely bár munkát jelent, mégis a legközvetlenebb aurát teremti meg védő és védett között - fogalmazott egykor számomra a világ egyik vezető politikusa.

A képzést ezért a minőségbiztosítási feladatokkal egyenértéken kezeli a menedzsment. Minden lehetőséget megragadok, hogy munkatársaim a világ élvonalába tartozó szakmai műhelyekben vehessenek részt képzéseken, bizonyíthassák rátermettségüket. Az éves képzési terv legfontosabb része a képzések megtervezése, amely mellett magam is gondot fordítok arra, hogy ne csak a szenvtelen professzionalizmus, hanem a személyes, négyszemközti beszélgetések is építsék szolgáltatásaink hírnevét. Nagyon hasznosnak tartanám, ha Budapest adhatna otthont egy, a magánbiztonsági szolgáltatók számára biztosított képzési központnak, hiszen a jogi különbözőségek nem jelentősek, a gyakorlat pedig közel azonos.

Felhasznált irodalom

[1] COESS, (2008): La participation de la sécurité privée á la sécurité génerale en Europe. CoESS – Confederation of European Security Services. Livre Blanc, Décembre 2008. Institut National des Hautes Etudes de Securite, France.”Vhite paper Private Security”. A dokumentumot francia nyelven dr. Finszter Géza, az Országos Kriminológiai Intézet munkatársa bocsátotta rendelkezésünkre, elérhető az In-Kal Security 2000 Kft. archívumában.

[2] 2005 évi CXXXIII. Törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

[3] BÖKÖNYI István - JÁRMY Tibor: A magánbiztonság főszereplője: a biztonsági őr. Jegyzet az In-Kal Security 2000 Kft. Biztonsági őr (Vagyonőr, Testőr) szakképzésének hallgatói számára. Budapest, 2009. ISBN: 978-963-06-7951-0

[4] DEUTSCH, William: About.com Guide to Business Security http://bizsecurity.about.com/od/physicalsecurity/u/Phys_sec_path.htm#s2

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Gyarmati Gábor
gyarmati.ornamentum@gmail.com

A NEM HALÁLOS FEGYVEREK KIKÉPZÉSI RENDSZERÉNEK HELYZETE A MAGYAR HONVÉDSÉGBEN

Absztrakt

A Magyar Honvédség szervezetében, felépítésében, feladatrendszerében az elmúlt évtizedekben jelentős változások mentek végbe. Az új típusú kihívások, új képességeket, modern technikákat, eljárásokat és speciális felkészülést igényelnek. Néhány nem halálos fegyver alkalmazása korábban is jelen volt a Magyar Néphadseregben később a Magyar Honvédségben is a kényszerítő eszközök közé sorolva (gumibot, gázspray, bilincs), igaz annak csak minimális jelentőséget tulajdonítva. Az új fogalomként jelentkező, nem halálos fegyverek köre azonban, ennél a pár eszköznél lényegesen nagyobb skálát ölel át. Az új eszközökre történő kiképzés új kihívásokkal állítja szembe az alkalmazókat.

Great changes took place in the last decades in the structure, tasks and organisation of the Hungarian Army. The new tasks require new types of capabilities, characteristic and modern techniques and training. Some non-lethal weapons were present in the old army structure (Hungarian people's army) and later in the Hungarian Army as implementation devices (truncheon, handcuffs, CS pray) but their importance were less significant. The variety of the new non-lethal weapons is much wider today than just the few that were mentioned above. Training for the new weapons demands new challenge for the trainers.

Kulcsszavak: *nem halálos fegyver, kiképzési rendszer, kényszerítő eszközök, katonai rendész, tömegkezelés ~ non-lethal weapon, Crowd and Riot Control, training, Civil Distrubances, Military Police*

„A békefenntartás nem a katonák
feladata, azonban csak a katonák
tudják azt elvégezni.”
(Dag Hjalmar Agne Carl Hammarskjöld)[1]

A Magyar Honvédség feladatrendszerének átalakulását követően megjelentek, olyan igények, mely nem a cél teljes fizikai megsemmisítését, hanem annak csak harcképtelenségének, üzemképtelenségének kiváltását igényeli. A béketámogató (béketeremtő, békefenntartó, katonai rendész, tartományi újjáépítő) feladatok sok esetben a műveleti területen történő békés megoldásokat követelnek meg. A modern nem halálos fegyverek, és a hagyományos fegyverek kombinált alkalmazása lehetővé teszi az új elvárásoknak történő megfelelést. Ezen eszközök alkalmazása mind egyedi eszközként, mind más fegyverrendszerekkel együtt történő alkalmazása számos új problémakört vet fel. A hagyományos és nem halálos fegyverek együttes alkalmazása során a cél fizikai megsemmisítésén kívül megvalósulhat annak harcképtelenné tétele, mely során a cél további kezelése, annak szakszerű kontrol alá vétele további feladatokat ró a végrehajtó állományra. A szakszerű és biztonságos végrehajtás alapvető feltételei a megfelelően kiválasztott és magas szinten kiképzett személyi állomány és a rendelkezésükre álló modern technikák alkalmazásának összhangja.

A kiképzési rendszernek, rendszereknek érzékenyen kell reagálni a technikai fejlesztések által kínált lehetőségekre.

A 1996-ban Szomáliában „United Shield” műveletben szerzett tapasztalatokat felhasználva az Amerikai Egyesült Államok Védelmi Minisztériuma létrehozta a Nem Halálos Eszközök Fejlesztési Programját (JNLWD)[2]. [1] A program célja a nem halálos technológiák fejlesztésének támogatása, a meglévő eszközök vizsgálata, a kiképzési rendszerek kidolgozása, továbbá a területet érintő adatok feldolgozása.

A program eredményeképpen egy komplett rendszer alakult ki a nem halálos fegyverek alkalmazásának területén a kutatás-fejlesztéstől a rendszerbeállításon keresztül az alkalmazás és a rá történő kiképzésig bezárólag, nem kis szerepet szánva a tapasztalatok feldolgozására. [2]

A nem halálos technológiák alkalmazásának előnyei elsősorban a katona rendész tevékenységek során jelentkeznek. A katonai rendész járőr (MP)[3]és a tömegkezelés (CRC)[4] tevékenységek során számos élő erő ellen alkalmazható (AP)[5] nem halálos technológia támogathatja az eredményes feladat végrehajtást. A technikai eszközök ellen bevethető nem halálos fegyverek (AM)[6]eredményesen alkalmazhatóak az ellenőrző áteresztő pontokon (CP)[7]és az objektumvédelemben.

A Magyar Honvédség 1995 óta vesz részt olyan missziókban (Ciprus, KFOR, EUFOR, stb.), ahová katonai rendész tevékenységekre kell felkészülni. Ezen missziókban tömegkezelési gyakorlatot is meg kell szerezni a résztvevőknek, ennek értelmében a Magyar Honvédségben jelenleg a nem halálos fegyverek alkalmazására – elsősorban katonai rendész tevékenységekre - történő kiképzések végrehajtásra kerülnek. Természetesen a hazai katonai

[1] Dag Hjalmar Agne Carl Hammarskjöld (1905-1961) az ENSZ második főtitkára
[2] Joint Non-Lethal Weapon Directorate - JNLWD
[3] MP- Military Police
[4] CRC – Crowd and Riot Control
[5] AP – Anti Personel
[6] AM – Anti Material
[7] CP - Control Point

rendészek is ki vannak képezve a saját felszerelésükbe tatozó eszközök használata (gumibot, bilincs, gázspray).

Ahhoz, hogy egy feladatra történő felkészülés eredményes legyen a következő fő követelményeknek kell teljesülni:

- *Követelményrendszer, szabályzatok, utasítások, kiképzési okmányrendszer,*
- Megfelelő minőségű és mennyiségű eszköz,
- Megfelelő minőségű és mennyiségű oktató eszköz (gyakorló eszközök, oktató eszközök, tablók, oktató filmek, stb.)
- Kiképzett kiképzők, szakemberek, tanácsadók,
- Írott és elektronikus oktatási segédanyagok,
- Fizikailag és szellemileg megfelelően felkészített oktatandó állomány,
- Infrastruktúra.

Különbséget kell tenni a feladat végrehajtásának előírásai és az arra történő kiképzés előírásai között.

Elsősorban vizsgáljuk meg a rendelkezésre álló szabályzatokat, utasításokat, amelyek előírják a tevékenység követelményrendszereit.

Jelenleg a Magyar Honvédségben a nem halálos fegyverek kiképzésével foglalkozó szabályzatok száma rendkívül kevés. Önálló szabályzat, utasítás nem foglalkozik a témával, a meglévő utasítások is csak érintőlegesen foglalkoznak a témakörrel.

Az Amerikai Egyesült Államok hadserege például már 1985-ben kidolgozott, és alkalmazott egy civil zavargások kezelésének módszereire vonatkozó szabályzatot,[8]mely tartalmazza a nem halálos fegyverek alkalmazására vonatkozó ismereteket. [3]

A Magyar Honvédségen belül a nem halálos fegyverek alkalmazásának ismereteit külön szabályzat nem tartalmazza.

A legátfogóbb képet a nem halálos fegyverekről, azok definíciójáról, csoportosításáról és a hozzá kapcsolódó ismeretekről a Zrínyi Miklós Nemzetvédelmi Egyetemen, Nem halálos fegyverek, egyetemi jegyzetében találhatók[9]. Ebben a jegyzetben már a nemzetközileg elterjedt szakmai terminológia, csoportosítás és ismeretek találhatók. [4]

A nem halálos fegyverek alkalmazására vonatkozó szabályzók jelenleg a Magyar Honvédségben a következők:

- Az általános katonai kiképzés kézikönyve I.-II. kötet[10]
- Békefenntartó kézikönyv[11]
- A Magyar Honvédség szolgálati szabályzata[12]
- Az adott misszió SOP[13] nem halálos fegyverekre vonatkozó alkalmazási feltételek,
- MH Katonai közelharc – kézitusa szakanyag (alapfok)[14]

A fenti szabályzók a különböző tevékenységi körök (katonai rendész, tömegkezelés, stb) során az alkalmazás szabályait írják elő, tehát mit, hogyan kell szabályosan végrehajtani, felvázolják az alapelveket, viszont nem vonatkozik a kiképzési követelményekre.

Az általános katonai kiképzés kézikönyve I. kötet, mint nevében is jelzi az általános kiképzési témakörökkel foglalkozik, és mivel a nem halálos fegyverekre történő kiképzés nem

[8] FM 19-15 Civil Distrubances, HQ Department of The Army Washinton, DC, 1985
[9] Bartha Tibor: Nem halálos fegyverek, Egyetemi jegyzet, E-jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Kar, Budapest 2009
[10] A HM Hadműveleti és Kiképzési Főosztály Kiadványa 2008
[11] A MH SZFP kiadványa 2004
[12] Ált/23, A Magyar Honvédség kiadványa 2007
[13] SOP - Standard Operating Procedure - Szervezési Működési Szabályzat
[14] A HM Hadműveleti és Kiképzési Főosztály Kiadványa 2007

sorolható az általános ismeretanyagok közé, ezért természetes, hogy ebben a kézikönyvben csak érintőlegesen foglalkoznak a témával. Az V. fejezet *A nem háborús műveletek* fejezetben taglalja az ellenőrző áteresztő ponton (CP) szolgálatot teljesítő személyek feladatát az ellenséges szándékú kisebb és nagyobb erejű csoportok megjelenése esetén. [5]

Békefenntartó kézikönyv III. fejezete, 8 pontjában a zavargások ellenőrzésére tér ki, de a tömegkezelés tevékenységet nem szabályozza. A X. fejezetben a Felkészítés és kiképzés részben is csak az kerül tárgyalásra, hogy milyen ismereteket kell elsajátítani. Érdekesség, hogy ebben a fejezetben sem található tömegkezeléssel kapcsolatos követelmények. [6]

A Magyar Honvédség szolgálati szabályzatának VIII. fejezete foglalkozik a kényszerítő eszközök használatának szabályaival, kizárólag a katonai rendész járőr tekintetében. [7]

Az adott misszió SOP-a tartalmazza a tömegkezelések során betartandó szabályokat, a nem halálos fegyverek alkalmazásának alapelveit.

MH Katonai közelharc – kézitusa szakanyag (alapfok) foglalkozik nem halálos fegyver alkalmazása során alkalmazható gyakorlati fogásokkal, igaz ez csak a botra vonatkozik, mely viszont jól alkalmazható a gumibotra, fém teleszkópos taktikai botra egyaránt, de ebben a szakanyagban nem kizárólagosan a nem halálos alkalmazási mód az elsődleges. Más nem halálos fegyverekkel, mivel az nem szigorúan kötődik a katonai közelharchoz természetesen nem köteles a szakanyag foglalkozni. [8]

A fentiek meghatározzák (igaz nagyon kis mértékben), hogy mikre kell felkészíteni, mit hogyan kell végrehajtani a katonai rendész tevékenység során, viszont nem rögzítik a kiképzés feltételeit (téma/tárgykör, óraszükséglet, kiképzők, stb.). További problémát jelent, hogy a nem halálos fegyverekkel külön egyik szabályzó sem foglalkozik, azokban csak nyomokban található utalás rá. Problémaként merül fel, hogy a szövetségi rendszerben történő együttműködés esetében, a szövetséges erők alkalmazásában lévő nem halálos fegyverekről megszerezhető ismeretekkel sem foglalkoznak.

Az élet nem áll meg, a katonákat fel kell készíteni a feladatuk ellátására. Ahhoz, hogy eredményesen fel lehessen készülni, a kiképzést jelenleg a következő szabályzók szerint töltik meg tartalommal:

- Kiképzési program a MH külföldi katonai kontingensébe beosztott békefenntartó-, fegyvernemi- és szakmai katonái és alegységei kiképzéséhez[15],
- A missziós tapasztalatok és a külföldön tanult tiszt, tiszthelyettesek megszerzett tapasztalatainak alkalmazása,
- Rendőrségi szakemberekkel, kiképzőkkel történő együttműködés.

Kiképzési program a MH külföldi katonai kontingensébe beosztott békefenntartó-, fegyvernemi- és szakmai katonái és alegységei kiképzéséhez-ben jelenik meg először a tárgykör óra elosztás. A problémát az jelenti, hogy az 1994-ben megjelent kiképzési program óta eltelt 17 év során olyan nagymértékű változásokon ment keresztül a nem halálos fegyverek köré épülő technikai és feladatrendszer, ami megköveteli ennek a kiképzési rendszernek a frissítését.

Érdekesség, hogy a felhasználható irodalmakként a „ a Magyar Köztársaság Fegyveres Erőinek Szolgálati Szabályzatát, A Katonai Rendészeti Utasítást és a Magyar Köztársaság Rendőrsége Szolgálati Szabályzatát”adja meg.

A katonai rendész járőr és a tömegkezelés tekintetében az 5. tárgykör óraszámai is (teljes állomány részére 2 óra, a rendész alegység részére 10 óra) nagyon kevésnek tűnnek. [9]

[15] Nytszám: 381/451 Kiképzési program a MH külföldi katonai kontingensébe beosztott békefenntartó-, fegyvernemi- és szakmai katonái és alegységei kiképzéséhez, A MH Szárazföldi és kiképzési főszemlélőség kiadványa, 1994

A missziós tapasztalatok és a külföldön tanult, szolgált tiszt, tiszthelyettesek megszerzett tapasztalatainak alkalmazása továbbra is nagy jelentőséggel bír, mivel már kiforrott, folyamatosan innovatív rendszerekkel megismerkedve, bővíthetik a kiképzés hatékonyságát.

A rendőrségi szakértők, kiképzők bevonása rendkívüli hatékonysággal bír, mivel a katonai rendész tevékenységek jellege nagyban megfelelője a rendőrségi tevékenységeknek. Továbbá előnyt jelent, hogy hazánkban a rendőri tapasztalatok az utóbbi években jelentősen bővültek (mind negatív, mind pozitív hasznosítható tapasztalatokkal), és a hadműveleti területen végrehajtható formájának, így az ilyen módon megszerzett ismeretek, rendkívül értékesek.

A kiképzés során végrehajtott gyakoroltatás, módszerek, normák, mind a fent említett módon kerülnek megalakításra.

A fentiekből kiderül, hogy a Magyar Honvédség nem rendelkezik egységes kiképzési követelmény rendszerrel a nem halálos fegyverek tekintetében.

Nincs kidolgozva kiképzési rendszer a:

- különböző eszközök használatára, különböző szituációkban egyénileg,
- különböző eszközök használatára, különböző szituációkban, alegység kötelékben,
- különböző eszközök kombinált alkalmazására, különböző szituációkban, alegységkötelékben,
- továbbá a fentiek életszerű kombinációira.

A kérdés persze lehet, az hogy szükséges egy ilyen rendszer?

Az 1995 óta megjelent békefenntartói feladatok egyenes ágon hozták az igényt a katonai rendész feladatok magas szintű ismeretére. Az ilyen irányú feladatok ellátására rendkívül sok fajta nem halálos fegyvert lehet és kell alkalmazni.

Mondhatnánk, hogy a Magyar Honvédségben kevés ilyen fegyver van, azokra meg egyszerű a kiképzés.

A valóság egy kicsit bonyolultabb!

Jelenleg rendszerben és alkalmazásban számos olyan nem halálos fegyver és a CRC tevékenységkor alkalmazott felszerelés található meg, melyek száma nem nevezhető kevésnek.

A katonai rendész felszerelésében megtalálható a gumibot, a gázspray. A balkáni missziókban a CRC feladatok ellátására rendelkezünk Remington Express Magnum típusú sörétes puskákat, nem áthatoló lövedékekkel, 40 mm-es DT-10 típusú gránátvetőket, különböző tömegoszlató, barikádromboló gránátokkal. A rövidesen alkalmazásra kerülő 40 mm-es MK-19 automata gránátvető, és a AK modernizáció során megjelent lövészfegyverre integrálható 40 mm-es gránátvető is alkalmas nem halálos lövedékek kilövésére.

A lista még nem végleges mivel az innovációra való hajlam megvan a katonai felső vezetés részéről, viszont az anyagi háttér korlátai meghiúsíthatnak számos kezdeményezést.

Abban az esetben, ha a Magyar Honvédség raktáraiban, „elfekvőben” lennének fém taktikai teleszkópos botok, abban az esetben már csak szakmailag felelős döntésekre lenne szükség, hogy azt a missziókban alkalmazhassák, ezzel növelve a hatékonyságot és az egyszerűbb feladatellátást.

A fenti fegyverek önálló alkalmazása és azok kombinált alkalmazása is megköveteli egy jól kidolgozott kiképzési rendszert.

A rendőrség által alkalmazott eszközök területén is hasonló a helyzet. A felső vezetés döntésének függvényében tudnak csak modern, magas színvonalú technikákat alkalmazni.

A 2006. évi tömegoszlatásos események ráirányították a figyelmet a rendőrségen belül is az alkalmazott technikák jogilag rendezett felhasználására vonatkozólag.

Az igazságügyi és rendészeti miniszter rendeletben[16] bővítette az alkalmazható nem halálos fegyverek listáját például a változtatható méretű (összetolható) rendőrbotokkal és az elektromos sokkolókkal, egyértelművé téve az addig alkalmazott rendőrbot fogalmát. [10] Már csak az adott eszközök rendszerbe állítása szab határt a fém taktikai teleszkópos botok elterjedésének. Szakmailag megalapozott döntés és felelősségvállalás a felsőbb döntéshozói szinteken és megfelelő kiképzési rendszer működtetése az alkalmazói szinteken a későbbiekben hatékonyabb, kevesebb sérüléssel járó tevékenységeket eredményezhet.

Végül levonhatjuk a következtetést, hogy megérett a Magyar Honvédség arra, hogy a nem halálos fegyverek, kiképzését átgondolja, megtegye a szükséges lépéseket annak kidolgozására.

Mik azok, amelyek jó alapot szolgáltatnak a nem halálos fegyverek alkalmazására történő kiképzési rendszer kialakítására?

- A már fent említett, meglévő szabályzók,
- A rendőrségnél alkalmazott szabályzatok, a megszerzett tapasztalatok alkalmazása, átdolgozása a katonai sajátosságoknak megfelelően,
- A NATO és az ENSZ által alkalmazott rendszerek, szabályzatok alkalmazása,
- Az adott nem halálos fegyver gyártója által kifejlesztet, ajánlott kiképzési rendszer átvétele, felhasználása,
- A hazai szakember állomány missziós és külföldi tanulmányokon megszerzett tapasztalatának feldolgozásából származó tudáshalmaz (melyek feldolgozása szükséges)

Nagy figyelmet kell fordítani arra, hogy a nem halálos fegyverek alkalmazása során számos variáció lehetséges:

- hagyományos fegyverek kiegészítése más hagyományos fegyverekkel melyek alkalmazhatók nem halálos fegyverként,
- hagyományos fegyverek kiegészítése nem halálos fegyverrel,
- több különböző elven működő nem halálos fegyverek kombinációja.

A fenti kiinduló adatok eredményes feldolgozása során figyelembe kell venni, hogy:

- a megalkotni kívánt rendszer folyamatosan modernizálható legyen (a jelentkező kihívásoknak, az újonnan megjelenő technológiáknak megfelelően).
- a kialakított rendszer a kiképzendő állományra a lehető leggyorsabb kiképzést tegye lehetővé a legnagyobb hatékonyság mellett.

Ahhoz, hogy egy kiképzési rendszer, egy szabályzat tartalma egyértelmű legyen ahhoz szükséges egy egységes szakmai nyelvezet terminológia kialakítása, bevezetése, mert a különböző eljárások, eszközök más-más elnevezése nagymértékben megnehezíti a hatékony munkát (pl.: kényszerítő eszközök – nem halálos fegyverek, vipera – fém taktikai teleszkópos bot, stb.).

A hatékony kiképzés elképzelhetetlen a professzionális ismeretekkel rendelkező kiképzők nélkül. Egy modern kiképzés keretén belül már nem elégséges, hogy valakit beküldenek egy foglalkozási jeggyel a foglakozásra, hogy tartsa meg azt. A kiképzőknek hiteles ismeretekkel kell rendelkezni. A nemzetközi gyakorlatban a kiképzőket is kiképzik, nem elég az eszköz alkalmazásának ismerete, azon felül kell ismernie, többek között a kiképzés felépítését, a hatékony elsajátíthatóság elérését. Nagyon jó példa erre a nemzetközileg bevált Felhasználó (User) – Kiképző (Instructor) – Mester kiképző (Master Instructor) kiképzői rendszer, mely hasonlít a Magyar Honvédségben alkalmazott osztályba soroló rendszeréhez, csak lényegesen egyszerűbb.

[16] 32/2009. (VIII.19) IRM rendelet

Egy jól kidolgozott kiképzési rendszer a nem halálos fegyverekre (mely része lehet a katonai rendész kiképzési rendszernek) nagyban elősegítené a hazai és missziós tevékenységek hatékonyságát, jogilag rendezné az esetleges nem kívánatos események tisztázását, rendezését.

Felhasznált irodalom

[1] Bartha Tibor: A nem háborús katonai műveletekben alkalmazható nem halálos fegyverek, KARD és TOLL - Válogatás a hadtudomány doktorandusainak tanulmányaiból, Honvédelmi Minisztérium oktatási és Tudományszervező Főosztály kiadványa 2044/1 pp.: 63-64 http://jnlwp.defense.gov/about/history.html, (letöltve: 2011.12.04.)

[2] http://jnlwp.defense.gov/about/purpose.html, (letöltve: 2011.12.04.)

[3] *FM 19-15 Civil Distrubances*, HQ Department of The Army Washinton, DC, 1985 http://www.globalsecurity.org/military/library/policy/army/fm/19-15/CH9.htm, (letöltve:2011.12.03.)

[4] Bartha Tibor: Nem halálos fegyverek, Egyetemi jegyzet, E-jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Kar, Budapest 2009

[5] Az általános katonai kiképzés kézikönyve I.-II., A Honvédelmi Minisztérium Hadműveleti és Kiképzési Főosztály Kiadványa 2008

[6] Békefenntartó kézikönyv, A Magyar Honvédség Szárazföldi Parancsnokság kiadványa, 2004

[7] Ált/23, A Magyar Honvédség szolgálati szabályzata, a Magyar Honvédség kiadványa 2007

[8] MH Katonai közelharc – kézitusa szakanyag (alapfok) A Honvédelmi Minisztérium Hadműveleti és Kiképzési Főosztály Kiadványa 2007

[9] Nyt. szám: 381/451 Kiképzési program a MH külföldi katonai kontingensébe beosztott békefenntartó-, fegyvernemi- és szakmai katonái és alegységei kiképzéséhez, A MH Szárazföldi és kiképzési főszemlélőség kiadványa, 1994

[10] Az igazságügyi és rendészeti miniszter 32/2009. (VIII. 19.) IRM rendelete

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Horváth Attila
horvath.attila@zmne.hu

ADALÉKOK ÉS MEGVÁLASZOLATLAN KÉRDÉSEK A SZERETFALVA–DÉDA VASÚTVONAL ÉPÍTÉSÉNEK TÖRTÉNETÉHEZ

Absztrakt

A politikai elit és a közvélemény öröme az 1940. augusztus 30-án aláírt második bécsi döntést követően nem volt teljes, mert a Budapest-Kolozsvár-Sepsiszentgyörgy vasútvonal Apahida és Nyárádtő közötti szakasza Romániá területén maradt. Ez volt az ún. Gőring has, vagy Gőring zsák. A Székelyföld vasúti összekötettés nélkül maradt, ezért például ellátási és katonai szempontból veszélyes helyzet alakult ki. Nem volt más megoldás mint új vasút vonalat építeni. A szerző a rövid tanulmányban összefoglalja a Szeretfalva Déda vasútvonal kijelölésének fontosabb, politikai, katonai és műszaki vonatkozásait.

In 1940 according to Second Vienna Award Hungary received back North Transylvania. The political elite and general public pleasure was not complete because of Budapest-Nagyvárad-Kolozsvár-Sepsziszentgyörgy section of railway line between Apahida and Nyárádtő remained in Romania. This was so-called Goring's abdomen or Goring's sack. The Székely land left railway connection, so military and public point of view situation was very dangerous. There was no other solution that to build a new railway line on Hungarian territory. The author issues a brief study designation of Szeretfalva Déda railway line is more important political, military and technical aspects.

Kulcsszavak: *terület visszacsatolások, vasúti közlekedés, katonai szállítások ~ reannexation, rail transport, military transport*

A MÁSODIK BÉCSI DÖNTÉS HATÁSA AZ ÉSZAK–ERDÉLY VASÚTHÁLÓZATRA

Bevezető

Az első világháború kitöréséig a vasútépítés „hőskora" gyakorlatilag Magyarországon is befejeződött. A trianoni békeszerződés a magyar vasúti hálózatot is kedvezőtlenül érintette, mivel egy organikusan kiépített hálózatot szerkezetét módosították mesterségesen. Mivel a teljes területi revízióról nem beszélhetünk az első bécsi döntéssel kezdődő 1938 őszén kezdődő terület visszacsatolásokkal sem állt helyre a korábban egységes magyar vasúti hálózat. Állami beavatkozásra volt szükség a korábban megszakított vasútvonalakon a forgalom helyreállítása érdekében, illetve MÁV a Szeretfalva és Déda között egy új vasútvonal építésére kényszerült. Erre azért volt szükség, mert az 1940. augusztus 30-án a bécsi Belvedere palotában kihirdetett második bécsi döntés vasúti közlekedési szempontok helyett a német gazdasági érdekeket vette figyelembe. Ez a rövid – a teljesség igénye nélkül – tanulmány elsősorban a vasútvonal építésének szükségességével és körülményeivel foglakozik.

A feszült magyar-román viszony megoldása: a második bécsi döntés

A Magyar Királyi Honvédség 1939 márciusában a kedvező nemzetközi helyzetet kihasználva megszállta a trianoni békeszerződéssel elcsatolt Kárpátalját. Ezt követően az amúgy is feszült magyar–román viszony tovább romlott. 1940 május végétől a határ mindkét oldalán ismételten számottevő csapatmozgás kezdődött. A magyar kormány 1940. június 27-én olyan határozatot hozott, hogy amennyiben Románia teljesíti a Szovjetunió ultimátumát, vagyis átadja Besszarábiát és Észak-Bukovinát, akkor érvényt szerez a magyar területi követeléseknek. Augusztus elejére a két ország közötti politikai feszültség szinte tapinthatóvá vált és katonai felvonulás már olyan méreteket öltött, hogy a háború kitörésének veszélye reálissá vált.

A vitás kérdések rendezése érdekében 1940. augusztus 16-án Turnu-Severinben (Szörényvárott) kezdődő tárgyalások augusztus 24-én zátonyra futottak és megszakadtak. Augusztus végére Magyarország a román-magyar határ közelében összevont három hadsereget és a Fővezérség közvetlen alakulatokat, több mint 550 000 ezer katonát. Ezzel szemben a magyar felderítési adatok szerint a román hadsereg Erdélyben 16 gyaloghadosztályt, 2,5 lovashadosztályt 3 hegyi-, 1 gépkocsizó- és erőddandárt vonultatott fel Erdélyben.[1] A kétoldalú tárgyalások kudarca után a háború kitörése elkerülhetetlennek látszott. Ezt támasztja alá az is, hogy Werth Henrik gyalogsági tábornok a Honvéd Vezérkar főnöke 1940. augusztus 23-án délután kiadta az irányelveit a Románia elleni támadó hadműveletek megindítására. A kiadott parancsoknak megfelelően a magyar csapatok augusztus 27-re már elfoglalták a kijelölt megindulási körleteiket, amikor német és olasz diplomácia vezetői augusztus 30.-ra –valószínűleg román kérésre – Bécsbe rendelték a magyar és a román külügyminisztert és megfigyelőként gróf Teleki Pál miniszterelnököt.[2]

A diplomáciai lépés nem véletlenül történt, hiszen a nagyhatalmak közül elsősorban Németországnak, de Olaszországnak sem állt érdekében, hogy Magyarország és Románia között komoly fegyveres konfliktus törjön ki. Ezért a megoldás érdekében a politika és a

[1] Horváth Csaba: A második bécsi döntés és katonai jelentősége. Egyetemi jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem kiadványa. Budapest, 2001. 41. p.

[2] gróf Teleki Pál (Budapest, 1879 – Budapest 1941) neves geográfus, egyetemi tanár. A két világháború közötti magyar politikai élet egyik meghatározó alakja. A miniszterelnöki posztot kétszer töltötte be. Először 1920. július 19. és 1921. április 14-e között vezette a kormányt. Az első királypuccs után távozni kényszerült a posztjáról. 1941. február 16-tól ismét miniszterelnök lett 1941. április 3-án öngyilkosságot követett el, mert ellenezte Magyarország részvételét Jugoszlávia lerohanásában.

diplomácia történetben jól ismert divide et impera azaz „oszd meg és uralkodj!" elvet alkalmazták. Ugyanis a német birodalmi szempontok nem csak a háború elkerülését, hanem a magyar-román feszültség életben tartását is megkövetelték. A második bécsi döntés olyan szempontból is fontos, maradéktalanul sikerült a német politikai érdekeket érvényesíteni, vagyis a határozatban konzerválták a magyar–román ellentéteket. Mindez úgy sikerült elérni, hogy sem a magyar sem a román fél nem lehetett maradéktalanul elégedett a német és olasz közbelépés eredményeivel miközben mindkét ország külpolitikai mozgástere csökkent.

A román diplomácia minden lehetőséget kihasznált annak érdekében, hogy a gazdasági érdekeire hivatkozva Erdélyben a lehető legnagyobb területet tartson meg. Ilyen szempontból nem lehet véletlennek tekinteni, hogy a MICA bányavállalat aranybányainak 80%-a Romániában maradt, ugyanis a vállalkozás részvényeit még a bécsi tárgyalások előtt Hitler helyettesének, Herman Göringnek a testvére kapta meg.[3]

A Torda környéki gázlelőhelyekkel kapcsolatban is hasonló szempontok érvényesültek. A döntőbírósági ítélet meghozatalánál a „döntőbírák" a német gazdasági érdekek miatt megnyugtatóbbnak látták, ha a tordakissármási földgázmező továbbra is román fennhatóság alatt marad. A később ezt a területet a magyar közvélemény nagyon gyorsan „Göring-öbölnek", vagy „Göring hasnak" nevezte el. Egyértelmű, hogy a német politikai, és gazdasági megfontolások sokkal inkább befolyásolták a döntőbíróságot, mint a közlekedési szempontok. A földgáz lelőhelyekkel együtt ugyanis a Budapest – Nagyvárad – Kolozsvár – Sepsiszentgyörgy vasútvonal Apahidtól délre Tordakenderes – Székelykocsárd –Marosludas – Nyárádtő közötti vonalszakasza az országhatáron kívül esett. Emiatt a Székelyföldnek az ország többi részével nem volt közvetlen vasúti összeköttetése. A korabeli közlekedési viszonyok között közúton nem lehetett megoldani teljesen Székelyföld bekapcsolását az ország társadalmi és gazdasági vérkeringésébe.

A második bécsi döntés értelmében a Magyarországnak ítélt területekről a román hatóságokat és hadsereget 14 nap alatt kellett kivonni. A határozat 1.§ és 2. §-sa értelmében határ helyszíni kijelölésével, illetve a román kiürítéssel és a magyar bevonulással kapcsolatos kérdéseket román – magyar vegyes bizottságoknak kellett tárgyalnia. A határvonal számottevő kiigazítására, és ezáltal a vasúti közlekedés feltételeinek javítására ezeken a tárgyalásokon még reális lehetőség sem nyílt.

A megszakított vonalszakaszon, - a nemzetközi szerződésen alapuló – az un. rendes vasúti forgalom is csak nehezen különleges rendszabályok életbeléptetése mellett indult el.[4] A vasúti szállító kapacitás korlátozott lehetőségei miatt 1940 november elejétől, vagyis a Magyarországon át Romániába irányuló német csapat- és anyagszállítás negyedik hetében a megszakított vonalat is igénybe kellett venni az átmenő katonai forgalom lebonyolítása érdekében. A német hadvezetés ezt vonalat használhatta is az un. tancsapatok átszállítása után a Görögország és a Szovjetunió elleni felvonulás során. A szállítások ütemét a meglevő engedélyek és a jó szervezettség ellenére nyilvánvalóan csökkentette, hogy a megszakított vonalon a német katonavonatok irányítását a magyar katonai vasúti hatóságoktól az illetékes román szervek vették át.[5]

[3] Szavári Attila: Magyar berendezkedés Észak-Erdélyben (1940. szeptember – 1941. április). című munkájának pdf változata. Stúdium. pp. 272-303. URL cím: http://www.adatbank.ro/html/cim_pdf950.pdf

[4] Majdán János: A magyar határ két oldalán (1918–1996). Modernizáció–Vasút–Társadalom. Tanulmányok a vasútépítések hatásáról a XIX.–XX. században. ISZE Integral Kiadó Kft., Pécs. pp.153–162.

[5] Horváth Attila: A Magyar Királyi Honvédség szállító szolgálatának működési elvei és annak gyakorlati kérdései (1922–41). Kandidátusi értekezés. Budapest, 1997. 252. oldal.

DÖNTÉS A VASÚTVONAL ÉPÍTÉSÉRŐL

A Magyar Királyi Honvédség az 1940. szeptember 2.-ai román-magyar bizottsági tárgyalásokon kötött megállapodásnak megfelelően szeptember 5.-én kezdte meg a bevonulást Észak-Erdély területére. A bevonulásban a korábban felvonultatott magyar haderő kijelölt alakulatai vettek részt. Az időközben megkezdett leszerelések miatt a csökkentett létszámú hadsereg a bevonulást Észak-Erdélybe szeptember 13.-án fejezte be. A katonai bevonulást követően a visszacsatolt Észak-Erdélyi területeket be kellett kapcsolni az anyaország politikai-, közigazgatási-, gazdasági-, kulturális életébe. Ez rendkívül bonyolult szervezési munkát igényelt. A magyar kormányzat a katonai megszállást követően kiemelt feladatként kezelte a megfelelő közlekedési kapcsolat kialakítását az anyaországgal.

Mivel a román területen átmenő vasúti forgalom nem jelenthetett megnyugtató megoldást így más lehetőség nem maradt, mint egy új normál nyomtávolságú vasútvonal építése. A vasútépítést gróf Teleki Pál miniszterelnök szívügyének tekintette és helyszíni szemle jelentések alapján személyesebb részt vett a nyomvonal kijelölésében. A vonal kijelölése érdekében a helyszíni bejárást a Horthy Miklós kormányzó fia Horthy István[6] a MÁV elnöke mellett, Álgyay-Hubert Pál[7] a Kereskedelem- és Közlekedésügyi Minisztérium államtitkára vezették.[8] Az új vonal nyomvonalára három változatot vettek számításba. Az első két változat alapját Sajónagymaros – Marosludas vasútvonal a második bécsi döntés következtében zsákvonallá alakult Sajónagymaros – Mezőszentmihály vonalszakasza képezte. Az első variáns szerint Mezőszentmihály állomást kellett volna összekötni Szászrégennel, vagy Marosvásárhellyel. A második variáció szerint a meglevő keskenynyomtávú vonalak átépítésével Szászkelence – Kolozsnagyida – Szászrégen között épült volna meg az új vonal. Építési szempontból harmadik változat volt a legnehezebb, vagyis a Kolozsvár – Dés – Beszterce mellékvonal összekötése a székely körvasúttal.

Ennek a megvalósítása érdekében azonban Szeretfalva állomásából kiindulva új vonalat építeni 48 km hosszban Déda felé. Ezt a feladatot a székely körvasútig csak igen nehéz terepviszonyok között volt lehetett.[9] Annak ellenére, hogy az építészeti szempontok és gazdaságossági megfontolások a harmadik változat ellen szóltak mégis a Szeretfalva állomásból kiinduló vonal építése mellett döntöttek.

Ezen a vonalon ugyanis a szállítási távolság és a menetidő Sepsiszentgyörgy felé lerövidült. A katonai stratégiai szempontok is emellett a vonal létesítése mellett szóltak, ugyanis Magyarország határa Románia felé túlságosan közel esett az első két javaslat szerinti vonalhoz. Ez katonai, politikai és közlekedési aspektusból vizsgálva újabb veszélyeket hordozott magába. Az első világháború tapasztalatai igazolták és ezt alátámasztották a második világháború addigi eseményei is, hogy a határokkal párhuzamosan, vagy azok közelében „futó” vasútvonalakat szinte lehetetlen védeni.

---

6 Horthy István (Pola, 1904 – Ilovszkoje 1942) Horthy Miklós kormányzó fia. 1928-ban a Műegyetemen gépészmérnöki diplomát szerzett. 1938–40 között a MÁVAG vezérigazgatója. 1940. június 1-től a MÁV Igazgatóság elnöki tisztét töltötte be. 1942 február 19-től a kormányzóhelyettes. Nem támogatta Magyarország részvételét a németek oldalán a második világháborúban. 1942. augusztus 20-án a 2. magyar hadsereg repülő főhadnagyként halálos balesete szenvedett.

7 Álgyay-Hubert Pál: (Szeged 1894– Budapest 1945) 1918-ban építőmérnöki diplomát szerzett, 1924-ben műszaki doktorrá avatták. 1927-től Kereskedelemügyi Minisztériumban dolgozott. 1937–42-ben a Kereskedelemügyi- és Közlekedésügyi Minisztérium államtitkára. Szakmai tevékenysége elismeréseként a Magyar Mérnök és Építési-Egylet Hollán Ernő díjjal tüntette ki. Nevéhez fűződik a budapesti Boráros híd (ma Petőfi híd) tervezése.

8 A Szeretfalva–Déda vasút 1941–1942. A Magyar Királyi Kereskedelem- és Közlekedési Minisztérium kiadványa. Budapest, 1943. 1.o (a továbbiakban A Szeretfalva–Déda vasút…)

9 Horváth Ferenc: A MÁV utolsó nagy vasútépítési munkája Szeretfalva–Déda között 1940–1942-ben. Vasúthistória Évkönyv 1998. A MÁV Rt. Vezérigazgatóság kiadványa. Budapest, 1998. pp. 104–147.

A magyar kormány figyelemre méltó gyorsasággal döntött a vasútvonal építéséről. A vasútépítés történetével fogalakozó tanulmányok abban azonban tévednek, hogy az új vonallétesítésről szóló határozatot a második bécsi döntést követően néhány nap alatt, vagy más források szerint már szeptember 4-én meghozták. Erre a magyar kormányzati szerveknek és a vasúti hatóságoknak egyszerűen nem volt módja, mert a katonai bevonulás is csak szeptember 5-én kezdődött el. A román csapatok és közigazgatási szervek egy-egy területet a román – magyar vegyes bizottsági tárgyalásokon jóváhagyott ütemterv alapján ürítették ki, és a magyar csapatok ezt követően vonultak be. A román közigazgatási és katonai hatóságok által ellenőrzött területen, a tervezett vasútvonal körzetében egy magyar minisztériumi államtitkárnak, illetve a MÁV elnökének – főként a kormányzó fiának – szemleútja a magyar csapatok érkezése előtt okot szolgáltathatott volna a két ország közötti háborúra. Ezt pedig egyik fél sem engedhette már meg magának, mert az augusztus végi bécsi négyoldalú külügyminiszteri tárgyalások során Ribbentrop német külügyminiszter figyelmeztette a két országot arra, hogy a tengelyhatalmak a két ország közötti az esetleges fegyveres konfliktus kiszélesedését minden eszközzel megakadályoznak.

A Minisztertanács a második bécsi döntés után, a határozattal összefüggésben, vasúti közlekedéssel kapcsolatos kérdésekkel először 1940. szeptember 25-én foglalkozott. Ezen a kormányülésen született döntés arról, hogy az állam 1.200.000 pengővel támogatja a trianoni békeszerződés miatt korábban megszüntetett zsákvonalakon a vasúti forgalom újra indítását. A második bécsi döntés után a trianoni határmentén 5 megszakított vonalszakaszon 40 km hosszban kellett újra megteremteni a vasúti közlekedés feltételeit.[10] További kutatásoknak kell választ adni arra kérdésre, hogy mikor és miért jelölték ki valójában a végleges nyomvonalat. A neves földrajztudós Fodor Ferenc közvetlen munkatársa gróf Teleki Pál munkatársa és első kiemelkedő életrajzírója szerint a miniszterelnök a visszacsatolt Észak-Erdélybe szeptember 7-én utazott először.[11] Fodor Ferenc szerint a miniszterelnök az új vonalépítéssel és a vasútvonal nyomvonalának kijelölésének kérdéseivel 1940. szeptember 20-án kezdődő szemle útján foglalkozott.[12] A Minisztertanács 1940. szeptember 25-én tartott ülésen a Székelyföld vasúti összeköttetés kérdésével csak érintőlegesen foglalkozott a kormány. Az ülésen Varga József a Kereskedelem- és Közlekedésügyi Minisztérium vezetésével megbízott iparügyi miniszter arról tájékoztatta a kormányt, hogy megépítendő vasútvonal költségigényét csak a helyszíni viszonyok teljes ismeretében, az általános tervek elkészülte után lehetséges kialakítani.[13]

Az új vonal létesítéséről és a várható költségkeretről a Minisztertanács csak az 1940. október 4-én határozott. A kormány az építésre 28 millió-, a Szeretfelva – Dés vasútvonal „első-rangúsítására" 5,5 millió pengőt irányzott elő.[14] Ezen az ülésen a Kereskedelem- és Közlekedésügyi Minisztérium még mindig nem a megvalósult vasútépítésre kapott felhatalmazást. Ugyanis a Minisztertanács egy 41 km-es vasútvonal építését Szeretfalva és Magyaró vasútállomások között.[15] Azt a kérdést, hogy miért döntöttek a vasúti pálya 8-km-es meghosszabbításáról csak további kutatások után lehet válaszolni. Hamar kiderült, hogy a nehéz terepviszonyok miatt, hogy az első számvetések szerinti 28 millió pengő kevésnek bizonyul, így a beruházás költségkeretét többször emelték. Az új vonal építése végül is 72 milló pengő pénzügyi ráfordítást igényelt.[16]

[10] Magyar Országos Levéltár (a továbbiakban MOL): K-27. A Minisztertanácsi jegyzőkönyvek xerox másolata. 1940. szeptember 25.
[11] Fodor Ferenc: Teleki Pál. Mike és Társai Antikvárium kiadásában. Budapest, 2001. 218. p.
[12] Uo. pp. 220–222.
[13] MOL: K-27. A Minisztertanácsi jegyzőkönyvek xerox másolata. 1940. szeptember 25.
[14] MOL: K-27. A Minisztertanácsi jegyzőkönyvek xerox másolata. 1940. október 4.
[15] Uo.
[16] Ablonczy Balázs: A visszatért Erdély1940-1944. Jaffa Kiadó, Budapest, 2011. 177. p.

A VASÚTÉPÍTÉS ÉS A SZÉKELYFÖLD ELLÁTÁSA ÉRDEKÉBEN FOLYÓ KÖZÚTI SZÁLLÍTÁSOK

A megfelelő közlekedési kapcsolat kiépítését az anyaország és Észak-Erdély között megnehezítette az erdélyi úthálózat elhanyagolt állapota is. A kijelölt vasútvonal építésének előkészítésére, valamint a Székelyföld felé irányuló áru- és személyforgalom lebonyolítására a rendelkezésre álló közutak alkalmatlanok voltak. Ezért a Bethlen – Szeretfalva – Teke – Szászrégen 78 km hosszúságú gödörkavics-pályás útszakaszt alkalmassá kellett tenni az ország főútvonalainak napi átlagát messze meghaladó gépkocsi forgalomra. Az átvételt követően az útépítési munkálatok szinte azonnal megkezdődőtek és hetek alatt hengerelt makadám útpályát építettek és javították a gépjárműforgalom biztonságát.[17]

A közvetlen vasúti összeköttetés hiánya miatt veszélybe került a Székelyföld közellátása is. A személy- és áruforgalmat Beszterce és Szászrégen vasútállomások között közúton lehetett megszervezni. A magyar kormány úgy ítélte meg, hogy a Székelyföld téli ellátását csak akkor lehet biztonságosan megoldani, ha a szállítások irányítását, megszervezését és a hadsereg katonai közlekedési hatóságai végzik.[18]

A szállítandó anyagi készletek előteremtésével és a raktározás megszervezésével összefüggő feladatok elvégzésével a katonai közigazgatási szerveket bízták meg. A szállítások lebonyolításának irányítását a Besztercén települt 3. számú Központi Szállításvezetőség Kirendeltség végezte. A korabeli nyilvántartások szerint 1940. november 15. és 1940. december 15. között a személyek és a jelentős mennyiségű áru továbbítása 250 db. 3 t-s katonai-, 87 db. 2.5-3 t-s. 2.5-3 t-s MATEOSZ tehergépkocsit, valamint a MÁVAUT-tól 70-100 db gépkocsit illetve autóbuszt igényelt.[19] A szállításban résztvevő MATEOSZ gépkocsik fuvardíját a MÁV fizette ki. A szállításban résztvevő gépjárművezetők naponkénti igénybevételben voltak érdekeltek, mert a gépkocsi meghibásodásakor a javítás ideje alatt általányt nem fizették ki.[20] A honvédségi gépkocsioszlopok és a MATEOSZ gépjárművek alapvetően árut, míg a MÁVAUT gépkocsik személyeket szállítottak. A szállítási helyzetet az is bonyolította, hogy MÁVAUT tehergépjárműveit alkalmassá kellett tenni személyszállításra.[21] A szállításokat a közlekedési feltételek javulásával 1941. január 15-el, a Kereskedelem- és Közlekedésügyi Minisztérium által kijelölt polgári bizottság vette át. Ez azt jelentette, hogy 1941. január második felében a 3. sz. Központi Szállításvezetőség Kirendeltséget és a honvédségi gépkocsioszlopokat fokozatosan kivonták.[22] Ezt követően az ellátási szállításokat a polgári hatóságok vették át.

A korabeli közlekedés viszonyokat jól szemlélteti az is, hogy a Szeretfalva–Déda vonal építésének várható időszükséglete miatt a szállítási gondok enyhítése érdekében a Marosvásárhely–Kolozsnagyida keskeny-nyomtávolságú vonal azonnali meghosszabbítását határozták el Szászkelencéig. A hadsereg kijelölt vasútépítő alakulatainak munkájának köszönhetően az 1940. október 1-jén elkezdett építést gyorsan befejezték és keskeny-nyomtávolságú vonalszakaszt 1940. december 15-én megnyitották a forgalomnak.[23]

---

[17] Tóth László: Magyarország közútjainak története. A Közlekedési, Hírközlési és Vízügyi Minisztérium kiadványa. Budapest, 1995. 113. oldal
[18] Horváth Attila: i.m. 251. o.
[19] Hadtörténelmi Levéltár (a továbbiakban HL.) HM. Eln. III. Csoportfőnökség. 65.030/1940.
[20] HL. HM. Eln. III. Csoportfőnökség. 66.571/1940.
[21] HL. Vkf. Eln. VI/1. o. 5.849/1940.
[22] HL. HM. Eln. III. Csoportfőnökség. 6.607/1941.
[23] Zakariás Zoltán: Honvéd vasútépítők. Szekér Információs Rt. Kiadási hely és év nélküli. 100. o.

AZ ÉPÍTÉSI MUNKÁLATOKRÓL

A vasútépítés építési tapasztalatait a Kereskedelem- és Közlekedésügyi Minisztérium jelentése és a kiváló vasúttörténész Horváth Ferenc már hivatkozott munkája részletesen ismerteti. Ezért az építkezés csak néhány jellemzőjére hívom fel a figyelmet. A vasútépítés tervezése és előkészítése már 1940 őszén elkezdődött. Mivel a kijelölt térségről megfelelő térképek nem álltak rendelkezésre, ezért a tervezéshez Magyarországon először légi fényképeket használtak fel.[24] A nyomvonal kijelölése is nagyon gyorsan történt, a mérnökök és a földmérők 1941 januárjában kezdtek hozzá az ezzel kapcsolatos munkálatokhoz.[25] A tervezőmunka és építkezés közigazgatási engedélyezésének eljárása még be sem fejeződött, amikor az építőanyagok felhalmozása, a terep és egyéb munkálatok elkezdődtek.

A munkálatokat az ország vezető mérnökei irányították. Az építkezésen „csúcs időszakban" megközelítőleg 30 ezer munkás dolgozott, a teljes időtartam alatt átlagosan naponta 16 ezer ember munkájára volt szükség.[26] Az építkezés nagyságrendje vasút-építészeti szempontból is jelentős. Az építési anyagok hiánya és a csúszó mezőségi talaj megnehezítette az építők munkáját. Az új vonalon 2 850 000 m^3 földet emeltek ki, 4 állomást és 3 megállóhelyet építettek.[27] A vasúti szempontból magasnak számító 225 m szintkülönbség és a domborzati viszonyok miatt két alagutat is építeni kellett 496 m és 938 m hosszban.

Az új vonalon 1942. november elején már olyan tehervonatok is közlekedtek, amelyek a Székelyföld ellátását szolgálták. A Szeretfalva–Déda vasútvonalat a közforgalom számára Horthy Miklós kormányzó 1942. december 5-én nyitotta meg.[28] Előrevetítette Magyarország második világháborús tragédiáját, hogy az ünnepélyes átadást az építésről és a nyompályáról döntő vezetők közül sem gróf Teleki Pál miniszterelnök, sem Horthy István kormányzó-helyettes nem érhette meg. A Szeretfalva-Déda vasútvonal építése a vasút műszaki tanulságokon túl jó példát szolgáltathat arra, hogy a politikai vezetésnek milyen szempontokat kell érvényesíteni egy váratlan közlekedési zavar elhárítása érdekében, valamint arra nézve is hogyan kell biztosítani egy nagy beruházás megvalósításához szükséges társadalmi támogatást.

Felhasznált irodalom

[1] Ablonczy Balázs: A visszatért Erdély1940-1944. Jaffa Kiadó, Budapest, 2011.

[2] A Szeretfalva–Déda vasút 1941–1942. A Magyar Királyi Kereskedelem- és Közlekedési Minisztérium kiadványa. Budapest, 1943.

[3] Fodor Ferenc: Teleki Pál. Kiadó: Mike és Társa Antikvárium. Budapest, 2001.

[4] Dombrády Lóránd: Hadsereg és politika Magyarországon 1938–1944. Kossuth Könyvkiadó, Budapest, 1986.

[5] Horváth Attila: A Magyar Királyi Honvédség szállító szolgálatának működési elvei és annak gyakorlati kérdései (1922–41). Kandidátusi értekezés. Budapest, 1997.

[6] Horváth Attila: A vasúthálózat fejlesztésével támasztott katonai követelmények és tervek (1920–1941) Nemzetvédelmi Egyetemi Közlemények, Budapest 1998. pp. 313–327.

[24] Horváth Ferenc: i.m. 108. p.
[25] Ablonczy Balázs: i.m. 178.p.
[26] Uo. 178.p.
[27] A Szeretfalva–Déda vasút 1.p
[28] A Szeretfalva–Déda vasút 7. p.

[7] Horváth Csaba: A második bécsi döntés és katonai jelentősége. Egyetemi jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem kiadványa. Budapest, 2001.

[8] Horváth Ferenc: Változások a magyar vasúti hálózatban (1920–1945). Közlekedéstudományi Szemle. Budapest, 1996. 4. szám pp. 143–149.

[9] Horváth Ferenc: A MÁV utolsó nagy vasútépítési munkája Szeretfalva–Déda között 1940–1942-ben. Vasúthistória Évkönyv 1998. A MÁV Rt. Vezérigazgatóság kiadványa. Budapest, 1998. pp. 104–147.

[10] Majdán János: A magyar határ két oldalán (1918–1996). Modernizáció–Vasút–Társadalom. Tanulmányok a vasútépítések hatásáról a XIX.–XX. században. ISZE Integral Kiadó Kft., Pécs. pp. 153–162.

[11] L. Balog Béni: A magyar–román kapcsolatok 1939–1940-ben és második bécsi döntés. Megjelent a Múltunk Könyvek sorozat könyvkiadványaként. Pro-Print Könyvkiadó Csíkszereda, 2002.

[12] Szavári Attila: Magyar berendezkedés Észak-Erdélyben (1940. szeptember – 1941. április). című munkájának pdf változata. Stúdium. pp. 272-303. URL cím: http://www.adatbank.ro/html/cim_pdf950.pdf

[13] Szász Zoltán: Az utolsó magyar nagyvasút. História XXIV. évfolyam 8. szám, Budapest, 2002. pp. 15–17.

[14] Tóth László: Magyarország közútjainak története. A Közlekedési, Hírközlési és Vízügyi Minisztérium kiadványa. Budapest, 1995.

[15] Zakariás Zoltán: Honvéd vasútépítők. Szekér Információs Rt. Kiadási hely és év nélküli.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Prekup Zsolt
prekupz@szabolcs.police.hu

KÖVESSÜK A TRENDET AVAGY RENDSZERESÍTSÜNK-E .223 REMINGTON (5,56X45 NATO) KALIBERŰ GÉPKARÉBÉLYOKAT

Absztrakt

Az elmúlt időszak eseményei időszerűvé teszik, hogy a fegyveres testületeknél meglévő szolgálati lőfegyverek mellé speciális egységek tagjai (operátorai, felszámolói) számára újabbak kerüljenek rendszeresítésre. A világban, minden hátránya ellenére egyre inkább terjednek .223 Remington kaliberű lőszert tüzelő gépkarabélyok és ez által ezekhez gyártott képességnövelő kiegészítők is.

Last events made actually to adapt new regulation firearms for the special units of armed forces. In spite of all their faults and disadvantages carbine submachines guns - fireing .223 Remington caliber cartidges- and their accessories are spreading in the world.

***Kulcsszavak**: fegyveres testület, szolgálati lőfegyver, összehasonlítás, Terrorelhárító Központ (TEK) ~ police, guns of duty, comparison, Counter Terrorism Centre (CTC)*

VÁLTOZÁSOK

1999. március 12-én NATO tagország, 2004. május 01-től hazánk az Európai Unió tagja. Ezen két tagsággal együtt, álláspontom szerint, olyan jogosultságokat is szereztünk, amely az esetlegesen lefolytatandó rendszeresítési eljárásoknál is előnyt jelenthet.

A NATO tagsággal lehetőségünk nyílt a STANAG előírások (ajánlás) átvételére és alkalmazására, amelynek során természetesen figyelemmel kell lennünk lehetőségeinkre. A témához kapcsolódó a STANAG 4172 az 5,56x45 NATO lőszer egységesítéséről szól.

Az 5,56x45 NATO kaliberű lövészfegyverek egyre inkább terjednek és népszerűbbek lesznek. Mára már elmondható, hogy több ország tart hadrendben ilyen kaliberű lőfegyvereket, mint a 7,62x39 vagy 5,45x39 kaliberű gépkarabélyokat.

Az 5,56x 45 NATO kaliberű lőszerekről és az azokat használó lőfegyverekről már hihetetlen mennyiségű cikk jelent meg, részletesen elemezve annak hadihasználhatóságát, megállító erejét, ergonómiáját és még jó néhány szempontot figyelembe véve. Sokan kritizálják a lőszer stophatását, külső ballisztikai teljesítményét.

Egy tény viszont tagadhatatlan. Szinte minden lőszergyár kínálatában szerepel az 5,56x45 NATO (polgári életben .223 Remington elnevezéssel bíró) kaliber. Ezen változatosságot még tovább növeli a kaliberhez tartozó lövedékek százas nagyságrendet meghaladó változata.

Érdekességként megemlíthető, hogy a FÉG is foglalkozott ilyen kaliberű, de Kalasnyikov alapokon nyugvó gépkarabélyok tervezésével is. Az 1980-as évek végén tervezett NGM/NGV (Nagysebességű Gépkarabély Modernizált – Nagysebességű Gépkarabély Válltámaszos) típusú lőfegyvereket a HM Haditechnikai Intézet (HTI) is tesztelte, sorozatgyártásra anyagi okok miatt nem került sor.

Az elmúlt évek iraki és afganisztáni tapasztalatai jelentős lökést adtak a kézi lőfegyverek és a hozzájuk tartozó kiegészítők fejlesztéséhez. Az 5,56x45 NATO kaliber legelső és azóta is töretlen használója az USA különböző fegyvernemei, figyelembe véve az egyes tagállamok kevés jogszabályi megkötést tartalmazó szabad lőfegyvertartását, értelemszerűen itt található a legtöbb gyártó és innen származik a legtöbb innovációs fejlesztés is a lőszerrel, illetve az ezt használó lőfegyverekkel kapcsolatban.

Az elmúlt évtized hadi tapasztalatai azt mutatják, hogy a hadviselés egyértelműen az aszimmetrikus (gerilla) hadviselés irányába mutat. Ezen hadviselési mód szerint harcoló egységek (az elnevezés változatos – szabadságharcos, lázadó, gerilla, partizán) ellen a terrorellenes hadviselésre kiképzett alakulatok harcolnak a leghatékonyabban. Észlelhető, hogy minden állam a jövőben még nagyobb hangsúlyt szeretne fektetni a terrorelhárító alakulatokra, akik a legtöbb esetben városi körülmények között tevékenykednek (például az aszimmetrikus hadviselés iskolapéldájának tekinthető Mogadishuban is így történt).

A városi körülmények közzé tervezett kézi lőfegyverekkel kapcsolatban, főleg a gépkarabélyokkal szemben, a követelményrendszer megváltozott. Álláspontom szerint egy ilyen CQB (close-quarter battle [1]) gépkarabéllyal szemben az alábbi elvárások támaszthatóak:

A CQB harcra tervezett gépkarabély tudja:

- biztosítani a rendszer pontosságát 300 méter lőtávolságig
- biztosítani a rendszer hatásosságát a megfelelő lőszer használatával ugyanezen a lőtávolságon, személyi páncél ellen is

[1] CQB (Close-Quarter Battle) angol rövidítésen eredetileg beépített környezetben végzett katonai tevékenységet értettek, azonban mára már több jelentése is van. A CQB rövidítést használják manapság most már szinte minden rövid távolságon belül végrehajtott harccselekménnyel kapcsolatban, legyen az épületben vagy repülőgép fedélzeten végrehajtva, mivel ugyanolyan divatszóvá alakult át mint a „taktikai" (tactical) kifejezés.

- biztosítani a lövésfolyamat szakaszos vagy folyamatos ismétlését a megfelelő pontossággal
- biztosítani a kiegészítő eszközök ergonomikus elhelyezését (irányzékok, lámpák)
- biztosítani különböző hatékonyságú hangtompítók használatát
- biztosítani a lövész önvédelmét közelharcban is
- biztosítani kiegészítő fegyverek használatát – (sokkoló -fegyvergránát)
- biztosítani a kapáslövés lehetőségét a lövésznek
- biztosítani a szolgálati feladatok indokolatlan terhelés nélküli elvégzését, különböző kiegészítők pl.: taktikai lámpa stb. felszerelhetőségét
- A hadszíntérnek megfelelően az adott paramétereken belül – a modularitás elvét követve - változtatható legyen a csőhossza, esetleg a kalibere

TUDNÁNK-E ALKALMAZNI AZ 5.56X 45 NATO KALIBERŰ CQB GÉPKARABÉLYOKAT?

Erre a kérdésre legegyszerűbben úgy válaszolhatnánk, hogy igen. Sőt már kis számban ugyan, de a Magyar Honvédség 34. Bercsényi Különleges Műveleti Zászlóalj (KMZ) kötelékében, amely a kinn harcoló szövetséges erőkkel kompatibilis fegyver, nevesítve M4A1-es gépkarabély (1. kép) került rendszeresítésre[1].

1. kép. M4A1 gépkarabély
Forrás: www.combatgear.blog.hu (letöltve: 2011 04.05.)

Az eddigi tapasztalatok azt mutatják, hogy a fegyver teljesítette a vele szemben támasztott követelményeket. Ahogyan a fenti képen is látható, a gépkarabélyra kiegészítők egész sorát szerelték fel. Ezen kiegészítők a következőek:

- sínrendszer a kiegészítők felerősítésére
- az első vertikális markolat Magpul RVG
- Magpul PMAG tár
- E.O. TECH 552 optikai irányzék
- Magpul PTS CTR gyártmányú válltámasz és PTS markolat
- Surefire lámpa vertikális markolatra helyezhető kapcsolóval
- hőpajzs

A Különleges Műveletei Zászlóalj különleges műveleti erők (Special Operations Forces – SOF) csoportjába sorolhatóak, amelyek kiképzésükkel és modern fegyverzettel oldják meg feladataikat.

Magyarországon a másik SOF kategóriába sorolható egység a 2010. szeptember 01-jén alakult Terrorelhárító Központ (TEK)[2].

A Stockholmi Program ajánlásai szerint az EU-n belül jött létre szinte teljesen profil tiszta terror ellenes szervezet, a TEK. A terrorizmus szemszögéből tekintve munkájuk célja a terrorcselekmények megelőzése, felderítése, felszámolása, a cselekmény folyamatainak megismerése, körözött személyek elfogása és nemzetközi együttműködések, melyek keretein belül részvétel az Európai Rendőr Iroda (European Police Office - EUROPOL) és az Európai Rendőr Kollégium (European Police College - CEPOL) terrorizmus elleni nemzetközi munkájában.

Bár fegyverzeti anyagukat és technológiájukat folyamatosan bővíteni igyekszenek, egyes lőfegyvereik világszínvonalat (pl.:Unique Alpine TPG-1) képviselnek, de a hagyományos, 1990-es évekre jellemző SWAT fegyverzetet (HK MP5 és USP változatok) követik.

Úgy gondolom, tekintettel feladataikra és a közelmúlt eseményeire pl.: Líbiában kint rekedt magyar állampolgárok hazahozatalára) célszerű lenne azt a lépést megtenniük, mint amelyet a KMZ, - igaz hathatós USA segítséggel -, de megtett. Logikus fejlesztési irány lenne számukra egy CQB 5,56x45 NATO gépkarabély rendszeresítése, hiszen az ilyen feladatkörrel megbízott SOF egységek fokozatosan térnek át a 9x19 Parabellum lőszert használó géppisztolyokról az 5,56x45 NATO kaliberű gépkarabélyokra (Pl. a lengyel GROM).

Említést érdemel, hogy bár az 5,56x45 NATO kalibert használó gépkarabélyok rendszeresítésében a KMZ volt az első hazánkban, azonban a külföldi trendnek való megfelelést Magyarországon először az azóta megszűnt Vám és Pénzügyőrség Központi Járőrszolgálat Parancsnoksága írta ki 2007-ben [3]. Az akkori kiírásban már szerepelt, igaz .223 Remington kaliber megjelölésével, a Heckler und Koch G36K típusú gépkarabély (2.kép)

2. kép. HK G36 K gépkarabély
Forrás: www.heckler-koch.de (letöltve: 2011 09.05.)

Úgy vélem, hogy a TEK részére, tekintettel feladataik sokszínűségére és veszélyességi fokára, indokolt lenne az áttérés. Néhány szempont, amely alátámasztja az 5,56x45 NATO lőszer (és a hozzá kapcsolódó fegyverrendszer) rendőri szempontból történő rendszeresítését:

- Különböző gyártók lőszer típusainak nagy száma, amelyet az adott rendőri feladathoz lehet kiválasztani (például az egyik tartaléktárban lövedékálló mellénnyel felszerelt elkövető semlegesítésére megfelelő lőszer)
- Rövid és közepes távon[2] is megfelelő hatótávolság (max. négyszáz méterig)
- A lőszer hihetetlen népszerűségéből fakadó és kellő marketinggel alátámasztott folyamatos fejlesztésének eredménye a kiegészítők hihetetlen mennyisége, amellyel a fegyvert személlyé szabottá lehet tenni ezáltal a kezelési ergonómiája megnövekszik

[2] A hatótávolság meghatározása főként lőszer paramétereitől (lőpor fajtája, lövedék külső kialakítása, lövedék anyaga és tömege) függ. Általános tapasztalatként elmondható, hogy a jelenleg legnépszerűbb lőszerek (pl. ATK Speer Gold Dot JSP) esetében a rövid távolság 0 métertől 50 méterig, a közepes távolság 50 métertől 150 méterig értendő.

A TÍPUSOK SOKSZÍNŰSÉGE

Tekintettel a lőszer népszerűségére, az ilyen fajtájú lőszert használó gépkarabélyok típusai széles spektrumot ölelnek fel.

Lentebb pedig következzen néhány figyelemre méltó típus nagyon rövid ismertetővel.

- M4A1 SOPMOD

3. kép. M4A1 SOPMOD gépkarabély
Forrás: www.combatgear.blog.hu (letöltve: 2011 09.10.)

A 3. Számú képen a Navy Seals által használt M4A1 változat látható [4]. Remekül megfigyelhető a CQB használatra tervezet és használt 9,5 inch hosszúságú cső Fast- attach system rendszerű Surefire FA556SA [5] típusú hangtompítóval (4. kép), amely segíti a rövid cső miatt kialakuló hangosabb lövészaj csökkentését.

4. kép. Surefire FA556SA hangtompító
Forrás: www.surefire.com (letöltve: 2011 08.14.)

- Ruger SR-556C

5. kép. Ruger SR-556C gépkarabély
Forrás: www.tactical-life.com (letöltve: 2011 09.01.)

Az ötös számú képen az USA-ban élő fiatalok kedvence (az ára miatt), a Ruger CQB feladatokra tervezett gépkarabélya [6] látszik, amely átépíthető .22 LR kaliberre is. Érdekessége a Magpul mellső markolat.

- Troy M7A1 SBR (6. kép)

6. kép. Troy M7A1 SBR gépkarabély
Forrás: www.tactical-life.com (letöltve: 2011 09.01.)

A Troy M7A1 SBR alapjait a Ruger SR-556 gépkarabély adja. A fegyveren elvégzett változtatások teljesen zárt helyen, rövid távolságon belül, városi környezetben végrehajtandó tűzharc sikeres megvívását segítik elő. Jellemző a nagyon rövid cső, amely jobb manőverezési lehetőséget ad a felhasználó számára, igaz a hatásos lőtávolság némi csökkentése árán.

- Bushmasters ACR – Magpul Masada

7. kép. Bushmasters ACR Magpul Masada gépkarabély
Forrás: www.tactical-life.com (letöltve: 2011 09.01.)

Az 5,56x45 NATO kaliberű gépkarabélyról bővebben ejtenék szót, mivel úgy gondolom, hogy ezen gépkarabély a fentiekben felsorolt kritériumoknak teljesen megfelel.

Az 7. képen látható gépkarabély tervezését 2007-ben fejezte be a Magpul Indrustriest. A Magpul fegyver kiegészítőket gyárt, leghíresebb termékük a tár aljára felhelyezhető kis műanyag fül, amely a tárak gyors elővételét hivatott elősegíteni. A fegyver sorozatgyártását a Bushmasters végzi ACR [8] (Advanced Combat Rifle) típusnév alatt.

A Magpul kiemelt fontosságot tulajdonított annak, hogy a lőfegyver modulárisan változtatható legyen. A tokalsórész (lower receiver) tartalmazza a tárfészket, az elsütőszerkezetet és a hátsó markolatot, amelyet két csappal lehet rögzíteni a tok felsőrészéhez (upper receiver).

A tok felsőrészből három verzió is készül, az egyik az 5,56x45 NATO kaliberhez, a másik a hazánkban rendszeresített 7,62x39 43 M lőszerhez, valamint az USA-ban egyre népszerűbb 6,8 SPC kaliberben. Ezen variációs lehetőségeken túl még a csövek és előagyak hosszát is lehet variálni (10,5; 14,5; 16,5; és 18 inch változatok).

Azt hiszem, ezen variációs lehetőségek hasznát nem kell kifejtenem. A tervezők szándéka szerint a fegyvert tábori körülmények között lehet egy kaliberről a másikra átszerelni, oly módon hogy csak a csövet, zárszerkezetet és a tokalsórészt kell kicserélni. Ergonómiája miatt jobb és balkezesek egyformán használhatják.

Egy nem régen megjelent közleményben az volt olvasható, hogy a Magyar Honvédség közel 10 évre elegendő 7,62x39 43M lőszerrel rendelkezik (bár az nem volt megadva mekkora éves lőszer felhasználás mellett) és közel 72000 db AK-val különböző típusokból.

A végletekig leegyszerűsítve egy ilyen fegyver előnyeit: legyen szó egy túszejtéssel járó bankrablás felszámolásáról (14,5 inch cső 5,56x45 NATO kaliber ATK Speer Gold Dot JSP lövedékkel), védett VIP személy biztosításáról (10,5 inch cső 5,56x45 NATO kaliberben) vagy felderítő feladat Afganisztánban (16,5 inch csőhosszúságú 7,62x39 43M kaliberben) történő elvégzéséről, a feladatot végrehajtó operátor vagy felhasználó a megszokott, megfelelő kiegészítőkkel ellátott fegyvert használja.

- Heckler und Koch 416

8. kép. HK 416 gépkarabély
Forrás: www.heckler-koch.de (letöltve: 2011 09.05.)

A 8. Képen látható HK416 (5,56 mm) [9] az USA különleges erőinél található M4/M16 típusú gépkarabélyok leváltására tervezték. Ugyanazt a gázdugattyús (short stroke) rendszert használja, mint az anyacég sikerterméke a G36 gépkarabély (amelyről volt már és lesz még szó), azonban ezen rendszer átültetése ésszerű volt az M4/M16 konstrukcióra. Működési rendszeréből adódóan ez a legmegbízhatóbb M4/M16 típusú fegyver.

2007 áprilisában, a HK416-ost választották a norvég hadsereg új szolgálati gépkarabélyának, összesen 8200 db-ot vásároltak belőle.

Ezen gépkarabélynak is létezik különböző csőhosszúságú (10,4 ; 14,5; 16,5 ; 20 inch /264, 368, 419, 508 mm/) verziója, de gyártják HK 417 jelzés alatt a 7,62x51 NATO kaliberű változatát is, azonban innen hiányzik a 7,62x39 43M kaliberű változat, amely ugyebár a Bushmasters ACR-hez képest visszalépés.

A fegyveren nem található kétkezes biztosító és ez szintén visszalépés a még a HK G36-hoz képest is.

- HK G36

9. kép. HK G36
Forrás: www.heckler-koch.de (letöltve: 2011 09.05)

10. kép. HK G36C
Forrás:www.heckler-koch.de (letöltve: 2011. 09.05.)

Ezen gépkarabély típusról joggal lehet állítani, hogy új szemléletet vitt a gépkarabély tervezés területére. A HK G36- nál [10] már könnyebb felsorolni azt, mi nem készült műanyagból. A tervezéskor szem előtt volt az ergonómia (jobb és bal kezesek számára is elérhető minden kezelőszerv) átlátszó tárak, beépített célzó optika.

A siker nem is váratott magára sokáig, 1995-ben rendszeresítette a Bundeswehr, majd 1998-ban Spanyolország (bár ők már használtak német gyökerű fegyvereket – CETME család).

A fegyver felkeltette figyelmét sok ország terrorelhárítással is foglalkozó egységének is. Kisebb megrendelések után két presztízs értékű megbízást kapott a HK. City of London Police és az US Capitol Police már használja a fegyvert, igaz ők a 2. képen látható HK G36 K és a 10. képen látható HK G36 C változatott rendelték meg.

A HK G36 négy féle változatban készül: HK G36 (9. kép) (480 mm csőhossz); G36 K (320 mm csőhossz ; G36 C(228 mm csőhossz); és rajtámogató változat(480 mm csőhossz Heavy csővel).

TALÁN KÖVETJÜK

A fent röviden ismertetett lőfegyvereket már sokféle szervezet, sokféleképpen használja. Úgy gondolom, tekintve a bekövetkezett jogszabályváltozásokat (pl. közbeszerzési törvény módosítását vagy az új rendőrségi szolgálati szabályzat) egyszerűbb folyamat lehet rendszerbe állítani egy új lőfegyver típust és lőszert. Hazánkban a Rendőrségnél rendszeresíthető kényszerítő eszközök típusairól és fajtáiról szóló, többször módosított 32/2009. IRM [11] rendelet mellékletének kiegészítésével már rendszeresíthető lenne az 5,56x45 NATO lőszer és az ilyen lőszert használó gépkarabély.

Felhasznált irodalom

[1] Egy magyar katona afganisztáni felszerelése
www.combatgear.blog.hu (letöltés: 2011 04.05.)

[2] 295/2010. Kormányrendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól

[3] Fegyverekre és fegyverzeti anyagokra a 228/2004 Kormányrendelet alapján lefolytatásra kerülő nyílt eljárásra
www.vam.hu (letöltés: 2011 08.27.)

[4] Cameron Hopkins: Colt M4A1 5.56 mm Carbine
http://www.tactical-life.com/online/special-weapons/colts-m4a1-556mm-carbine/
(letöltés: 2011 08.15.)

[5] Rifle/ Carbine Suppressors – 5,56 mm (.223 Caliber)
http://www.surefire.com/RifleCarbineSuppressors556mm223Caliber/
(letöltve: 2011 08.14.)

[6] Len Waldron: Ruger's SR-556C 5,56mm
http://www.tactical-life.com/online/guns-and-weapons/ruger%E2%80%99s-sr-556c-556mm/ (letöltés: 2011 09.01.)

[7] P.J.White: Troy M7A1 SBR forrás:
http://www.tactical-life.com/online/special-weapons/troy-m7a1-sbr-upgrade/
(letöltve: 2011 09.01.)

[8] Richard Mann: Multi-Mission ACR
http://www.tactical-life.com/online/tactical-weapons/multi-mission-acr/
(letöltés:2011 09.01.)

[9] Strumgewehre (Produkte)
www.heckler-koch.de (letöltés: 2011 09.05.)

[10] Strumgewehre (Produkte)
www.heckler-koch.de (letöltés: 2011 09.05.)

[11] 32/2009. IRM rendelet Rendőrségnél rendszeresíthető kényszerítő eszközök típusairól és fajtáiról

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Bottyán Zsolt
bottyan.zsolt@uni-nke.hu

IN-SITU LEVEGŐKÉMIAI ÉS LÉGKÖRFIZIKAI MÉRÉSEK A FAAM BAE-146-OS FEDÉLZETÉN: A SONATA PROJEKT – ELŐZETES EREDMÉNYEK

Absztrakt

A repülőgépes in-situ meteorológiai mérések rendkívül fontosak a levegőkémiai és felhőfizikai folyamatok vizsgálatához valamint ezek modellezéséhez egyaránt. Munkánkban a SONATA projekt keretében, 2011. augusztusában, a FAAM BAe-146-os kutató repülőgépének fedélzetén elvégzett légköri mérésekről számolunk be, melynek során a fontosabb üvegházhatású gázok, a nitrogén-oxidok, a szén-monoxid, a troposzferikus ózon koncentrációjának térbeli és időbeli alakulását vizsgáltuk, Olaszország és az Adriai-tenger felett. Bemutatjuk a repülőgépes mérésekre történő felkészülési folyamat elemeit, magát a repülőgépet, a konkrét repülési útvonalat és elvégezzük a repülési nap időjárási analízisét is. Tekintve, hogy a mért adatok kiértékelése jelenleg is folyamatban van, munkánkban bemutatjuk az eddig feldolgozott mérési eredményeket, a troposzférikus ózon és a nitrogén-dioxid koncentrációk térbeli és időbeli eloszlására vonatkozásában.

The airborne in-situ meteorological measurements are very important to examine and model the microphysical processes in the atmosphere. In our work we show the atmospheric airborne measurement of greenhouse gases, O_3, NO_2 and CO on the board of FAAM BAe-146 aircraft during SONATA project in August of 2011. We present the steps of the preflight procedures, the BAe-146 aircraft itself, the flight path and we give a meteorological overview for the day of flight. Since the measured data set are not yet processed completely we show some preliminary results in connection with spatial and temporal distribution of O_3 and NO_2 concentration over Italy and Adriatic See.

Kulcsszavak: *repülőgép-fedélzeti mérés, repülési terv, ózon, SONATA projekt ~ aircraft airborne measurement, flight plan, ozone, SONATA project*

ELŐZMÉNYEK

2011 tavaszán az EUFAR (European Facility for Airborne Research) hivatalos honlapján megjelent egy pályázat, melyben PhD hallgatók és egyetemi oktatók részére pályázati lehetőséget biztosítottak az olaszországi Pescara-ban megrendezésre kerülő, nyári repülőgépes levegőkémiai és légkörfizikai mérési kampányon történő részvételre.

Tekintve, hogy ebben az időszakban már kidolgozás alatt állt az Óbudai Egyetemmel közösen benyújtott TÁMOP pályázat (a pilóta nélküli repülőeszközök komplex repülésmeteorológiai biztosításának kidolgozása c. alprogrammal), melynek egyik fontos eleme in-situ repülőgépes meteorológiai mérések tervezése, végrehajtása és a mért adatok feldolgozása. Ezért, oktatóként megpályáztam a SONATA (School ON Aircraft Techniques for the studies of Atmospheric chemistry) projektet, tapasztalatszerzés céljából.

A sikeres pályázatom után felkészültem a 2011. augusztus 17-28 közötti elméleti oktatásra és a gyakorlati repülési program végrehajtására. A projektben történő részvételt minden hallgató számára teljes egészében az EUFAR finanszírozta.

ELMÉLETI KÉPZÉS A SONATA PROJEKT KERETÉN BELÜL

A kiutazást követő napon megkezdődött a különböző európai országokból érkezett résztvevők (meteorológusok, levegőkémikusok) elméleti felkészítése. Tekintve, hogy a projekt alapvetően repülőgép fedélzetén történő levegőkémiai mérések tervezéséről, végrehajtásáról szólt, az elméleti felkészítés a következő témákat érintette:

- Általános levegőkémiai (fotokémiai, kémiai) és légkörfizikai folyamatok áttekintése a légkörre vonatkozóan;
- Az éghajlatváltozás és a levegő kémiája;
- A troposzférikus ózon (O_3), nitrogén-oxidok (NO_x), szén-monoxid (CO) valamint az üvegházhatású gázok koncentrációjának méréséhez használt mérőműszerek elvi felépítése, használata és installációja;
- In-situ repülőgép-fedélzeti légköri mérések tervezése, gyakorlati végrehajtása, a végrehajtáshoz szükséges anyagi és eszközállomány beszerzésének pályázati lehetősége, rendszere;
- Pályázati lehetőség a FAAM (Facility for Airborne Atmospheric Measurements)-nál, korábbi mérési expedíciók végrehajtása, eredményei és tapasztalatai;
- A FAAM BAe-146-os repülőgépe, fedélzeti mérőberendezései, biztonsági előírások;
- A mért adatok utófeldolgozásához szükséges elméleti ismeretek és szoftverek.

A felkészítést a szakma elismert kutatói-oktatói végezték, akik a FAAM, University of Leeds, University of Aquila, Metropolitan University, Tokyo intézmények munkatársai és számos hasonló projektben vettek már részt.

GYAKORLATI KÉPZÉS: FELKÉSZÜLÉS A REPÜLŐGÉP-FEDÉLZETI MÉRÉSRE

A résztvevők a kurzus második napjától kezdve, három csoportban – az elméleti előadásokkal párhuzamosan – dolgoztak a gyakorlatban végrehajtásra kerülő repülési program tervének kialakításán. Ez a rendkívül komplex feladat igen komoly és széleskörű ismereteket kívánt meg a csoportokban dolgozó résztvevőktől, hiszen egy teljes repülési tervet kellett kidolgozni a kurzus utolsó napjaira időzített, a FAAM BAe-146 fedélzetén elvégzendő mérési kampányra vonatkozóan. A tervezett repülési idő 3 óra volt, melynek során a kívánt repülési pályán, a megfelelő repülési manőverek végrehajtásával, az installált mérőberendezések

felhasználásával kellett a programot végrehajtani úgy, hogy közben percre pontosan meg volt határozva szinte minden fontos művelet. Mindeközben, a fedélzeti információs rendszeren keresztül nyomon kellett követni a mért adatokat és a berendezések működését is. A kívánt repülési/mérési terv kidolgozásához szükséges feladatok a következők voltak:

- Az elvégzendő mérési feladat jól definiált meghatározása, különös tekintettel a vizsgálandó gázok jelentős koncentrációban várható megjelenésére (pl. hajók kéményéből származó szennyezőanyag nyomkövetése és ennek összetevőinek, azok koncentrációinak mérése kis magasságban az Adriai-tenger felett, tengeri olajfúró-tornyok feletti metán koncentráció mérése, felhőben levő felhőelemek (cseppek) méret-eloszlásának meghatározása, stb.);
- Az adott napra vonatkozóan egy részletes meteorológiai helyzetjelentés (briefing) készítése (naponként frissítve, ahogy közeledett a repülési dátum) különös tekintettel a mérendő légköri gázok koncentrációjának és az egyéb állapotjelzők várható alakulására. Ennek repülésbiztonsági és méréstechnikai jelentősége egyaránt fontos.
- A földrajzi, légköri és légi-közlekedési helyzet figyelembe vételével, egy repülési útvonal kialakítás-optimalizálás, melynek során meghatározandó pontról-pontra a repülési sebesség, a repülési magasság, a mérési manőverek típusa (pl. határréteg alatt és felett történő lépcsős repülési mód, adott emelkedési sebességgel végrehajtott profil-mérési mód, stb.), a műszerek esetleges repülés közbeni kalibrációs pontjainak helyzete, a levegőből történő mintavételek helyei és időpontjai.

Az első tervezett repülési napunk előtt egy nappal a FAAM BAe-146-os repülőgépe megérkezett Pescara repülőterére, így ennek a napnak a délutánját a gép fedélzetén töltöttük, hogy megismerkedjünk a valóságban is az installált mérőműszerekkel és kaptunk egy gyakorlati oktatást a biztonsági tudnivalókról, a fedélzeti információs rendszer működéséről (HORACE) valamint a fedélzeti kommunikációs rendszer használatát (INTERCOM) is begyakoroltuk. Ez utóbbi használata rendkívül flexibilis működést tesz lehetővé a fedélzeten dolgozó pilóták, kutatók, műszer-specialisták és légi utaskísérők között (pl. előre nem várt veszélyes szituáció bekövetkezése esetén, a kutatási program azonnali módosítása valamilyen hirtelen megjelent légköri jelenség vizsgálata esetén, vagy éppen a műszerek által mért adatok repülés közben történő diszkutálása esetén stb.).

Ezután a BAe-146 pilótáival véglegesítettük a repülési tervet, amit ők hivatalosan eljuttattak a légi irányítás felé. Megbeszéltük részletesen a repülési útvonalat, manővereket, melyek tervezésében a nagy tapasztalattal rendelkező személyzet komoly segítséget nyújtott nekünk.

A FAAM BAE-146-OS (G-LUXE) LÉGKÖRI KUTATÓ REPÜLŐGÉPE

A repülőgépes fedélzeti mérésekhez egy BAe-146-os, G-LUXE lajstromjelű – speciálisan légköri mérések végrehajtására átalakított – repülőgépet vettünk igénybe a SONATA projekt keretén belül (1. ábra).

1. ábra. A FAAM BAe-146-os légköri kutató repülőgépe a pescarai repülőtéren (a szerző felvétele)

A repülőgép egy utasszállító példány átalakítása során nyerte el végső formáját, melynek során alapvetően a belseje változott meg. A repülőgép fedélzetén két sorban, szabvány méretű konténerekben kerültek elhelyezésre a mérőműszerek és a hozzájuk tartozó segédberendezések (szivattyúk, gáztartályok, csővezetékek, kábelek stb.) (2. ábra). Közöttük kerültek kialakításra a kutatók és technikusok munkaállomásai (3. A. ábra).A fedélzeti mérőberendezések közül a projektben az alábbiak voltak installálva a repülőgépen:

- Lézerrel indukált fluoreszcencia berendezés (LIF) a nitrogén-dioxid (NO2), peroxi-nitrátok (PNs), alkil-nitrátok (ANs), salétromsav (HNO3), koncentrációjának mérésére [1];
- Aeroszol tömeg-spektrométer (AMS) a légköri aeroszol összetételének megállapításához [2];
- Üregrezonancia lecsengési spektroszkópia (CRDS) üvegházhatású gázok (CH4, CO2, NH3) koncentrációjának vizsgálatához [3];
- Ózon (O3) fotométer a troposzferikus ózon koncentráció meghatározásához;
- Vákuumos UV rezonancia fluoreszcencia spektroszkópia a szén-monoxid (CO) koncentráció vizsgálatához [4];
- Passzív aeroszol spektrométer (PCAPS-100) aeroszol részecskék érzékelésére, méret szerinti eloszlásának meghatározására (3. B. ábra);
- Kondenzációs mag-számláló (CPC) műszer (3. B. ábra);[5]
- Vízcseppek keverési arányát mérő műszer (LWLCP) (3. B. ábra);[6]
- Az aeroszol részecskék fényszórásának vizsgálatára alkalmas nefelométer (TSI Nephelometer 3573) (3.C. ábra).

2. ábra. FAAM BAe-146-os légköri kutató repülőgépének belseje, a repülés felkészülési fázisában
(a szerző felvétele)

3. ábra. A. (bal felső kép): a mikrofizikai munkaállomás a BAe-146 fedélzetén B. (jobb felső kép): a mikrofizikai berendezéseket tartalmazó függesztett konténer; C. (bal alsó kép): a nefelométer berendezést tartalmazó konténer a fedélzeten; D. (jobb alsó kép): a repülés koordinátorának munkahelye
(a szerző felvételei).

A FAAM BAe-146-os légköri kutató-repülőgépének fontosabb adatai az I. táblázatban láthatóak. Fontos megemlíteni, hogy a repülőgép rendkívül pontos robotpilótával és navigációs rendszerrel van felszerelve, így akár hosszabb ideig is képes a tenger felett minimálisan 50 láb magasan is repülni. A repülőgép alkalmas a troposzféra teljes körű (horizontális és vertikális) levegőkémiai és meteorológiai szondázására, hiszen a

hatótávolsága 3700 km és a csúcsmagassága 35.000 láb. Egy üzemanyag-feltöltéssel, mintegy 5 órát képes a levegőben maradni.

Személyzet	3 fő
Tudományos kutatók száma a fedélzeten	18 fő
Hosszúság	31 m
Magasság	8,4 m
Fesztávolság	26 m
Hajtóművek	4 Honeywell LF507-1H gázturbina
Maximális repülési magasság	35.000 láb
Minimális repülési magasság	50 láb
Hatótávolság	3700 km
Repülési sebesség a projektek során	200 kts
Rakomány	4000 kg tudományos műszerek

1. táblázat. A FAAM BAe-146 repülőgép fontosabb műszaki adatai

A SONATA PROJEKT REPÜLÉSI ÚTVONALA – BAE-146 FEDÉLZETI MÉRÉSEK

Az utolsó három napra és naponként egy csoportra tervezett repülést végül az utolsó napon, két csoportra bontva végeztük, mert az első tervezett repülési napon kormánymű hiba miatt a futópályáról fordultunk vissza a torony előtti állóhelyre.

4. ábra. A SONATA projekt keretében végrehajtott repülés útvonala 2011. augusztus 27-én és a repülés alatt felbocsátott ózon szonda helye, valamint trajektóriája és a főizobár-szintek

Az időközben megérkezett repülőmérnökök munkájának eredményeképpen, végül, a repülést 2011. augusztus 27-én hajtottuk végre, amely során az alábbi repülési útvonal mentén végeztük a méréseket (4. ábra). A repülési útvonal mentén szürke színnel a repülés aktuális magasságát ábrázoltuk, ahol a sárga nyilak a repülőgép mozgásának irányát jelzik a pályaív mentén.

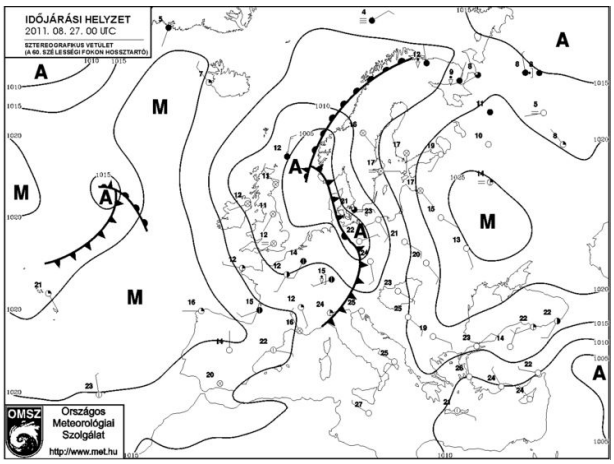
Idő1	Idő2	Esemény	Magasság (kft)	Rep. irány (fok)	Megjegyzés
100506		Video	0,15	166	Video rendszer indítása
100602		QNH	0,15	165	Magasságmérő beállítás 1008 hPa QNH
101854		**T/O**	**0,13**	**217**	**Felszállás Pescara-ból**
102055	102533	Profil 1	0,13----8,0	91	
102542	103711	Run 1	8,0	89	FL80
102639		**Kalibráció**	**8,0**	**87**	**Műszer kalibráció**
103712	104208	Profil 2	8,0----3,2	308	
104208	104525	Run 2	3,2	309	
104259		**Esemény**	**3,2**	**308**	**Hajók a terülen**
104536	104611	Profil 3	3,1----2,9	310	
104612	104719	Run 4	2,9	312	
104725	104747	Profil 4	2,8----2,7	307	
104748	105014	Run 5	2,7	310	
105046		**Esemény**	**3,6**	**354**	**AMS Probléma; emelkedés 5000ft-ra**
105200	105534	Run 6	5,2	353	
105535	110234	Profil 5	5,2----0,56	332	
110235	111638	Run 7	0,56----0,57	315	
110800		**Esemény**	**0,55**	**324**	**Elrepülés hajó felett**
111827	112152	Profil 6	0,68----2,6	129	
112153	112631	Run 8	2,6	153	
112637	112731	Profil 7	2,6----3,2	153	
112736	112755	Run 9	3,2	152	
112755	113420	Profil 8	3,2----10,1	154	
113430	115143	Run 10	11,0	156	FL110
115348	121027	Run 11	13,0	180	FL130
115528		**Kalibráció**	**13,0**	**180**	**Műszer kalibráció**
121000		**Esemény**	**13,0**	**254**	**Meteo. szonda felbocsátása**
121350	122550	Run 12	16,0	64	FL160
122550	124037	Profil 9	16,0----0,18	68	
124037		**Leszállás**	**0,18**	**217**	**Leszállás Pescara-ban**

2. táblázat. A repülési útvonal fontosabb manőverei és eseményei (a fontosabb műveletek félkövér betűvel jelölve)

Ahogyan az II. táblázatból kiolvasható, a kiindulási és érkezési repülőtér Pescara Airport (42º 25’ 54N; 14º 10’ 52E) volt és a tényleges repülési idő 10:18:54 UTC-től 12:40:37 UTC-ig tartott, ami 2:21:41 időtartamnak felelt meg. A repülési útvonal magassági adataiból jól látható, hogy a kelet felé történő felszállás után egy emelkedő profil-mérést végeztünk, majd a szárazfölddel közel párhuzamosan repülve, az Adriai-tenger felett egy süllyedő pályán végrehajtott több-lépcsős profilmérést hajtottunk végre. Ezután egy emelkedő profilmérés után alacsony magasságon repültünk a tenger felett, egészen megközelítve a Pó folyó torkolatát. Ezt követően ismét emelkedő profilmérést hajtottunk végre, majd a szárazföld belseje felé fordulva, állandó magasságon repültünk és két forduló után ismét a tenger felé érve, egy süllyedő profilmérés után leszálltunk. A 4. ábrán feltüntettük a repülés alatt felbocsátott ózon szonda három-dimenziós pályáját is a repülési útvonalhoz viszonyítva (jeleztük a főizobár-szinteket is). A szondát 12:10:00 UTC-kor bocsátották fel, hogy a fedélzeten mért ózon adatokat össze tudjuk hasonlítani a szonda által mért adatokkal (ebben az időpontban repültünk a szonda által is vizsgált régióban). A szonda felbocsátását a fedélzetről, műholdas telefonon keresztül koordináltuk a földi személyzettel.

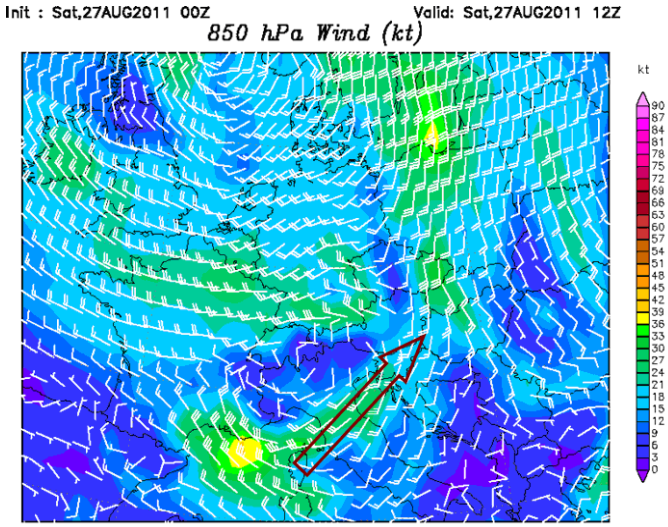
AZ IDŐJÁRÁSI HELYZET A PROJEKT REPÜLÉSI NAPJÁN

Az adott repülési napot (2011.08.27.) megelőzően, - már több napja - az Appenninek és a Földközi-tenger felett egy erős, nagy kiterjedésű magasnyomású légköri képződmény (anticiklon) helyezkedett el, mely az Északi-tenger feletti középponttal örvénylő ciklon K-i irányú mozgásának lassan teret engedve, fokozatosan EK-i irányban helyeződött át. A repülés napján középpontja már a Kelet-európai síkság felett volt (5. ábra).



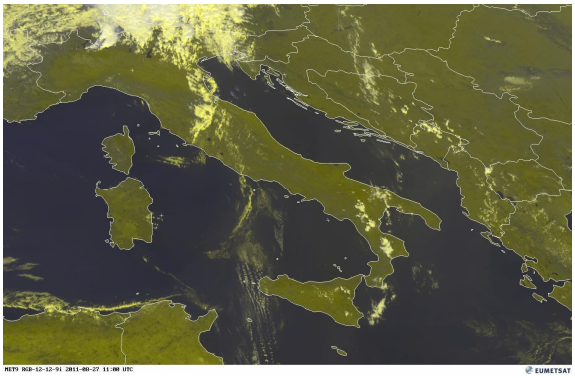
5. ábra. Az európai időjárási helyzet a SONATA projekt repülési napján, 2011. augusztus 27-én 00 UTC-kor
Forrás: Országos Meteorológiai Szolgálat

Ezzel egy időben, az említett ciklon hidegfrontja már az Alpok vonalában haladt és a meleg szektorban egy igen erős D-DNy-i, meleg száraz levegőt szállító áramlási mező alakult ki. Ennek eredményeképpen, Pescara repülőterén a kora délutáni órákban a hőmérséklet 40 ºC felé emelkedett és 10 méteren 8-10 m/s sebességű „forró", szinte sirokkó jellegű szél fújt. Az erőteljes pre-frontális áramlási rendszer az Appennini-félsziget felett jól látható az amerikai GFS globális időjárási modell adataiból, Közép-Európa térségére készített, 850 hPa-os nyomási szintre és a repülés napjára (12:00 UTC) érvényes szél-előrejelzési térképén is (6. ábra).



6. ábra. A repülési időpontra előrejelzett szélirány és szélsebesség (csomó) Közép-Európa felett a 850 hPa nyomási szinten (GFS globális modell). A nyíl az erőteljes hidegfront előtti áramlási rendszert mutatja
Forrás: http://www.wetterzentrale.de

Az időjárási helyzetből fakadóan, felhőzet a repülési régióban szinte alig volt, hiszen a rendkívül száraz troposzférában még a kialakuló konvektív cellák felszálló ágaiban sem történt markáns kondenzáció. Csak Olaszország ÉK-i területe felett lehetett a hidegfronthoz tartozó felhőzetet (Cu Cong., Cb) valamint a tagolt orográfia miatt kialakult hullámfelhőket a repülőgép fedélzetéről észlelni (7. ábra).



7. ábra. A felhőzet eloszlása a Közép-Mediterráneum felett 2011. augusztus 27-én, 11.00 UTC-kor
Forrás: EUMETSAT, www.eumetsat.int

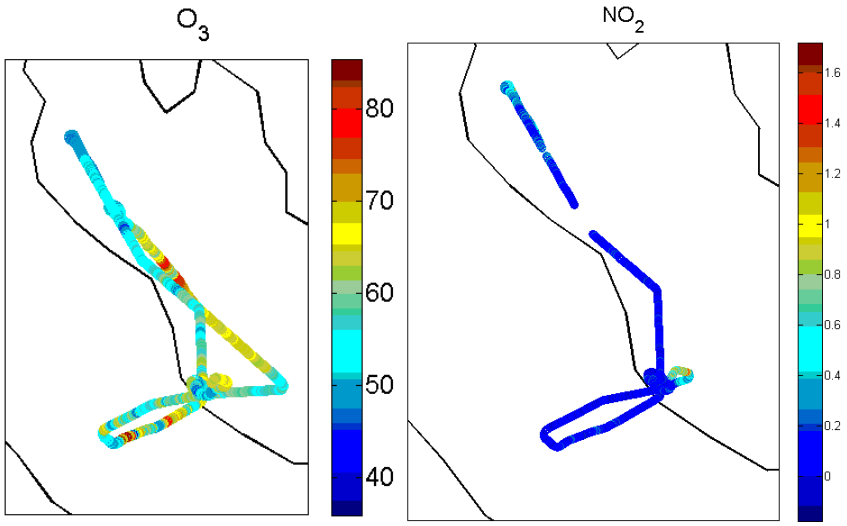
A REPÜLŐGÉP FEDÉLZETÉN MÉRT ADATOK ÉS ELEMZÉSÜK ELŐZETES EREDMÉNYEI

A repülés során – több más légköri összetevővel együtt – a troposzférikus ózon és a nitrogén-dioxid koncentrációját is folyamatosan mértük. A NO_2 esetében az átlagos koncentráció értéke 0,08 ppb volt 0,55 ppb maximális érték mellett. Az O_3 esetében pedig 57,12 ppb átlagos és 73,61 maximális koncentrációt mértünk (III. táblázat). Meg kell jegyeznünk, hogy műszer-probléma miatt a NO_2 koncentráció-mérést a repülés kezdeti szakaszában nem tudtuk elvégezni, ezért csak a Pó torkolatvidékétől vannak NO_2-re vonatkozó adataink.

Gáz	Átlagos koncentráció (ppb)	Minimális koncentráció (ppb)	Maximális koncentráció (ppb)
NO_2	0,08	0,01	0,55
O_3	57,12	42,73	73,61

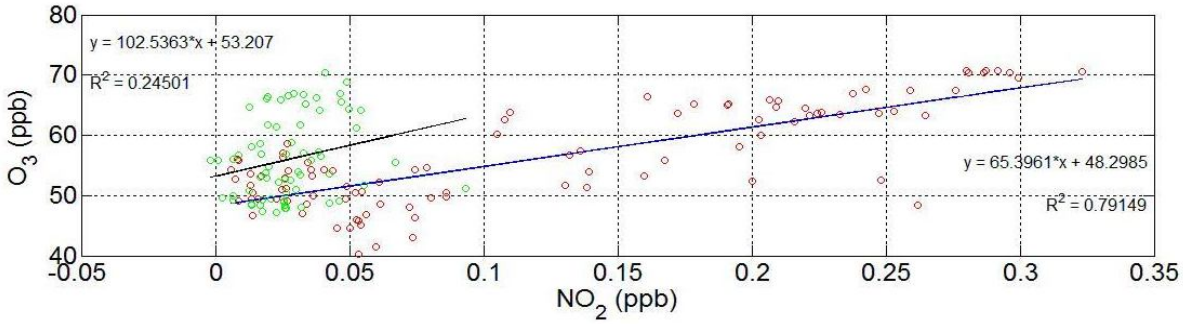
3. táblázat. A repülés során mért nitrogén-dioxid és ózon koncentrációk átlagai és szélső értékei

A mérés során tapasztalt koncentráció adatok a 8. ábrán láthatóak. Figyelembe véve az aktuális repülési útvonalat, megállapíthatjuk, hogy a magas NO_2 koncentrációkat az alacsony magasságok mellett (Pó völgy környéke és Pescara-hoz közel), míg az alacsony koncentrációkat a magasabb légrétegekben mértük, ami megegyezik az általunk várt eredményekkel. Az ózon esetében szintén az alacsony magasságú régiókban mértük a magasabb koncentrációt, ami a gáz keletkezési mechanizmusából fakadóan helytállónak mondható (8. ábra).



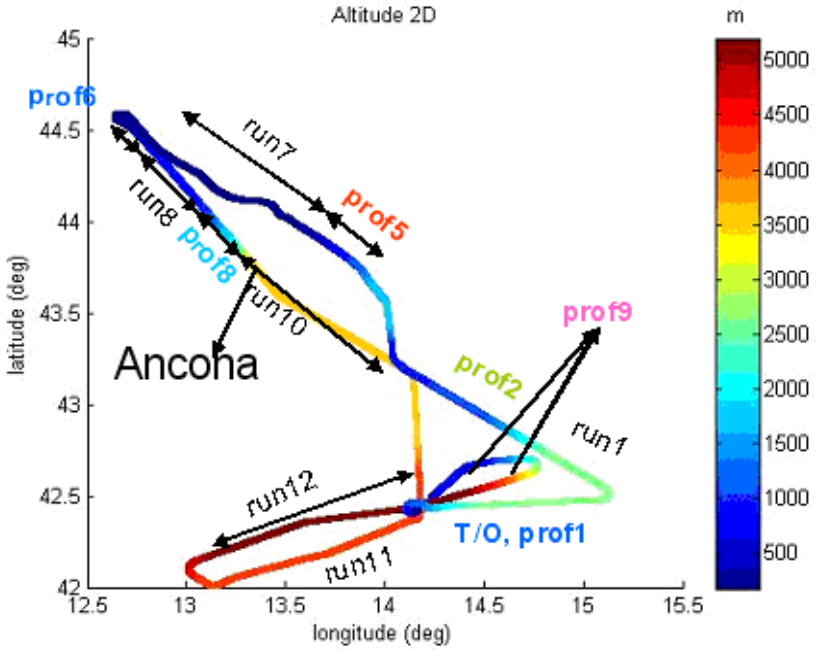
8. ábra. Az ózon (O3) és a nitrogén-dioxid (NO2) koncentrációjának alakulása a repülési útvonal mentén

A nitrogén-dioxid katalitikus szerepe a troposzferikus ózon-képződésben sokat tanulmányozott folyamat. Az NO_2 koncentrációjának növekedése fotokémiai reakciókon keresztül, a troposzférikus ózon koncentrációjának emelkedéséhez vezethet. Ennek a folyamatnak a dominanciája alapvetően a felszínhez közeli légrétegekben vehető észre. A repülési útvonal alacsonyabb (4200 méternél kisebb magasságú) mérési pontjain kapott koncentráció adatok pontdiagramon ábrázolva, jól mutatják ezt a működő mechanizmust (9. ábra). A NO_2 és O_3 koncentrációk között igen magas megmagyarázott variancia értékkel rendelkező lineáris kapcsolatot láthatunk, melynek statisztikai értelmezése alapján az ózon koncentrációjának alakulásáért - mintegy 80%-ban (R^2=0,79149) - a nitrogén-dioxid mennyisége a felelős. A magasabb légrészekben a kapcsolat erőssége ugyan jelentősen csökken, de így is kaptunk egy gyengébb lineáris trendet (R^2=0,24501).



9. ábra. Az ózon és a nitrogén-dioxid pontdiagramja. A zöld színű értékek a szárazföld feletti nagy magasságban (4200 méter felett) mért koncentráció adatokat, míg a pirosak az alacsonyabb magasságú értékeket jelölik

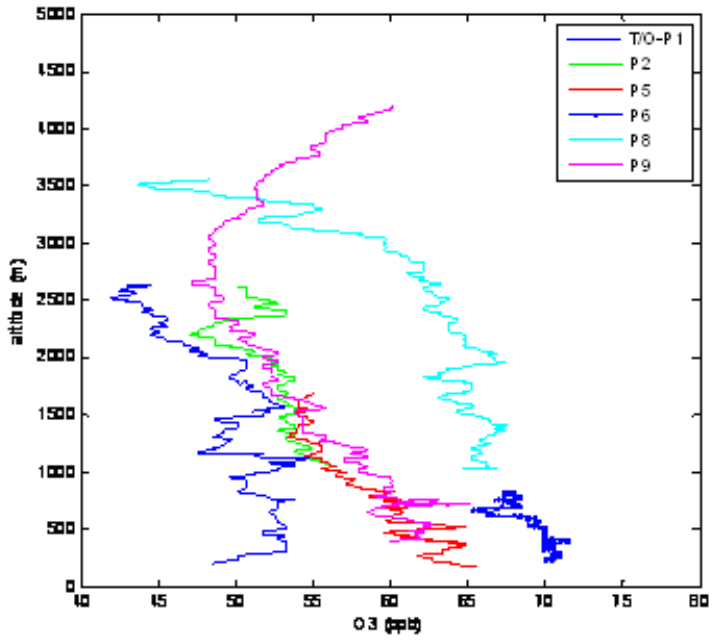
Természetesen rendkívül fontos a troposzférikus ózon magasság szerinti eloszlásának vizsgálata is. Éppen ezért – ahogyan a repülési terv kidolgozásánál említettük – a mérési útvonalba 9 ún. emelkedő/csökkenő profilmérést is végeztünk. A profilok térbeli (földrajzi szélesség, hosszúság és magasság szerinti) elhelyezkedését a 10 ábrán láthatjuk.



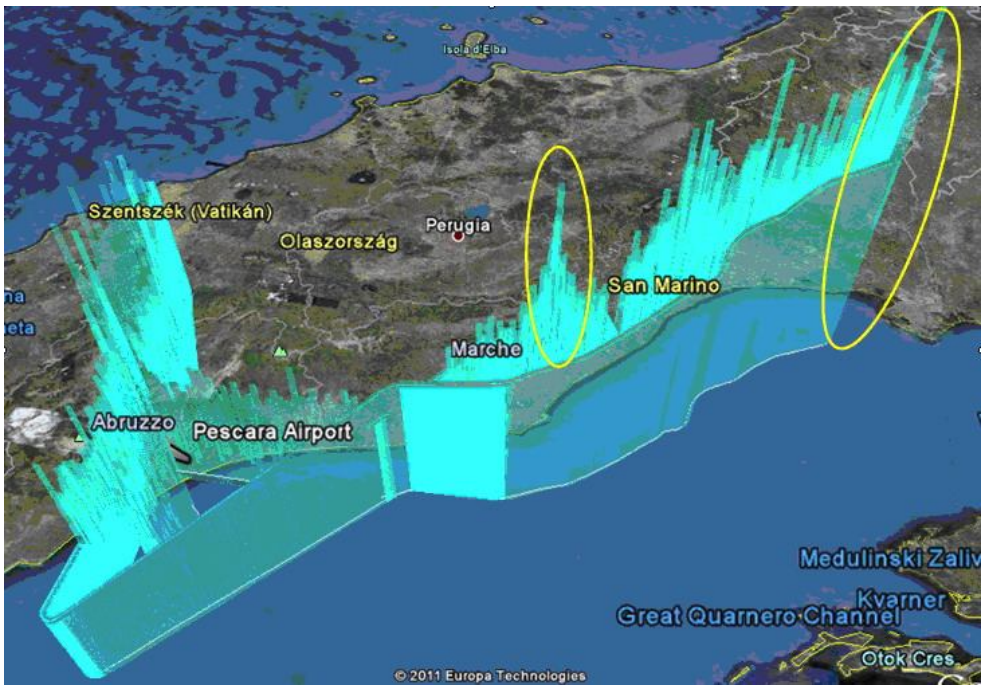
10. ábra. A repülési útvonal mentén végzett profil mérések térbeli eloszlása

Az elvégzett 9 profilmérés közül hatnak az eredményét mutatjuk be a 11. ábrán. Jól látható, hogy a planetáris határréteg felett az ózón koncentráció csökkenését tapasztaltuk, hiszen 800-1500 métertől a görbék a kisebb értékek felé hajlanak el. Ennek egyik oka, hogy a határréteg felett az átkeveredés kevésbé intenzív, így a felszín közelében képződő – gyakran antropogén eredetű nitrogén-dioxid - csak kisebb koncentrációban lehet jelen, ezért az ózon képződésében megfigyelhető katalitikus hatása is mérsékelt. Az ötödik (Ancona mellett) és a hatodik (Pó torkolathoz közel) profil estében jól észrevehető a magas koncentráció a felszín közelében (65 és 70 ppb) és a magassággal történő gyors csökkenés mértéke. Ugyanakkor mindkét esetben jelentős nagyrészt antropogén eredetű NO, NO_2 produkció is valószínűsíthető, amit az időjárási viszonyok felerősíthettek az adott vizsgált területen (Pó völgyből érkező és az Ancona-ból származó szennyezőanyag-advekció) (11. ábra).

Rendkívül jól észrevehető a nitrogén-dioxid koncentrációjában történt kiugrás is, mely szintén a Pó folyó torkolatvidékéhez közel és Ancona város felett rendelkezik helyi maximummal (12. ábra). Különösen jelentős lokálisan az Ancona-nál mért NO_2 koncentráció-növekedés, amit a DNy-ról (a szárazföld belseje felől) fújó erős szél advekciójának (transzportjának) is köszönhetünk. A Pó folyó torkolatának közelében, az NO_2 koncentráció szintén az advektív hatásnak köszönhetően érte el a magas értékét, melynek során jelentős mennyiségű nitrogén-dioxid (és más antropogén szennyező anyag) szállítódott a Pó folyó völgyéből (szárazföld) a tenger fölé.



11. ábra. A repülési útvonalon mért ózon koncentráció profilok. A vízszintes tengelyen az O3 koncentráció (ppb), a függőleges tengelyen a magasság (m) van skálázva. A színek az adott útvonalon mért adatokat jelentik



12. ábra. A NO2 gáz koncentrációjának eloszlása a repülési útvonal mentén. Kiugróan magas értékek Ancona és a Pó folyó torkolatvidékén (a helyi maximumok sárga ellipszisben jelölve)

A hatalmas mennyiségű mérési adat feldolgozása folyamatos, jelen tanulmányban csak egy kezdeti töredékét ismertettük meg. Amennyiben újabb eredmények lesznek, azokat a megfelelő szakmai médiumokban közzé tesszük.

ÖSSZEFOGLALÁS

Munkánkban a SONATA kurzuson végrehajtott elméleti és gyakorlati oktatásról számoltunk be valamint ismertettük a FAAM BAe-146-os kutató repülőgépének karakterisztikáit, a fedélzeten elhelyezett műszereket. Képet alkottunk a repülési terv kidolgozásának folyamatáról is és a rendkívül sokoldalú felkészítés után, a FAAM BAE-146 kutató repülőgép fedélzetén végrehajtott levegőkémiai és légkörfizikai mérésről valamint a megkezdődött adatfeldolgozásról.

Az előzetes adatfeldolgozás keretében ismertettük a troposzféra alsó felében mért O_3 és NO_2 koncentrációk vizsgálatából származó eredményeket és rámutattunk néhány fontos összefüggésre ezek között.

KÖSZÖNETNYILVÁNÍTÁS

Köszönetünket fejezzük ki az EUFAR vezetésének, a FAAM kutatóinak és a ZMNE rektorának, hogy támogatásukkal hozzájárultak a SONATA kurzuson történő részvételemhez és jelen tanulmány elkészültéhez.

Felhasznált irodalom

[1] Sadanaga, Y., Yoshino, A., Kato, S., Kajii, Y., Measurements of OH reactivity and photochemical ozone production in the urban atmosphere, Environmental. Science and. Technology. 39, (2005) pp. 8847-8852.

[2] Canagaratna et al: Chemical and microphysical characterization of ambient aerosols with the aerodyne aerosol mass spectrometer, Mass Spectrometry Review., 26, (2007) pp. 185-222.

[3] Liu, A.W., Kassi, S., Perevalov V., I., Hub, S., M., Campargue A.: High sensitivity CW-cavity ring down spectroscopy of N_2O near 1.5 μm. Journal of Molecular Spectroscopy, 254, (2009) pp. 20-27.

[4] Gerbig, C., Schmitgen, S., Kley, D., Volz-Thomas A.: An improved fast-response vacuum-UV resonance fluorescence CO instrument. Journal of Geophysical Report, 104., (1999) No D1, pp. 1699-1704.

[5] Geresdi, I.: Felhőfizika. Dialóg Campus Kiadó, Budapest-Pécs. 2004.

[6] Strapp, J., W., Schemenauer, R., S.: Calibrations of Johnson-Williams liquuid water content meters in a high-speed icing tunnel. Journal of Applied Meteorology, 21, (1982) pp. 98-108.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Dávidovits Zsuzsanna
davizsu@vipmail.hu

A VÍZVÉDELEM JOGI SZABÁLYOZÁSI RENDSZERE ÉS AZ IVÓVIZMINŐSÍTÉS SZABÁLYOZÁSA

Absztrakt

A víz az élő és élettelen környezet szerves része. Fontosságát és felhasználhatóságát már az ókorban felismerték, és hogy értékét óvják, már akkoriban bekerült a jogi szabályozások témakörei közé. A vízjog jelentősebb régebbi jogszabályainak rövid áttekintése után, a jelenleg is hatályban lévő jogszabályokat tanulmányozom át. Külön részben vizsgálom az ivóvíz minősítésére vonatkozó aktuális jogszabályokat.

The water in the animate and inanimate environment is an integral part. Its importance and usefulness has been recognized in the ancient world and to protect the value, already had been included among the subjects of legal regulation. After a brief overview of the major older legislations of the water-law I study the currently effective legislations. In a separate section the qualification of the current drinking water legislation will examine.

Kulcsszavak: *vízjog, vízgazdálkodás, Víz Keretirányelv, vízminősítés, vízvédelem ~ water-law, water management, Water Framework Directive, water rating, water protection*

RÖVID TÖRTÉNETI ÁTTEKINTÉS A VÍZVÉDELEM VONATKOZÁSÁBAN 2000-IG

A vízzel kapcsolatos jogi szabályozások, bármennyire is hihetetlenül hangzik, de már egyes ókori civilizációkban jelen voltak, mivel már akkoriban felismerték a vízzel kapcsolatos tevékenységek súlyát és fontosságát. Első sorban a vizek kártételei elleni védelemre és a vizek mezőgazdasági célú hasznosítására, a hasznosítás feltételeinek megteremtésére vonatkoztak ezek a szabályozások. Az első, törvénynek is tekinthető írásos dokumentumok még Mezopotámiából származnak, melyek az öntözőcsatornák létesítésekre és fenntartására vonatkoztak. A hazai vízjog kialakulása és fejlődése szempontjából azonban az ókori Róma vízépítészeti munkái és az ezekkel kapcsolatos vízjogi szabályozások jelentették az alapokat. Sok akkori jogrendelkezés szólt a vizekre vonatkozó előírásokról, azok tulajdonának, használatának szabályozásáról. Törvényi szinten megfogalmazták például, hogy a vizek, a folyók, vagy a kikötők olyan közdolgok közé tartoznak, melyek mindenkinek a rendelkezésére állnak és annyit használnak belőlük, amennyit csak akarnak - azaz a vizet senki nem veheti kizárólagosan a saját tulajdonába. Az első hazai, írásos vízjogi rendelkezések, dokumentumok már az 1100-as években megjelentek a „Corpus Juris Hungarici", azaz a Magyar Törvénytár köteteiben. Ezen rendelkezések főleg a tógazdaságok és a halászhelyek adományozására vonatkoztak. A Magyar Törvénytárban aztán IV. Béla idejében az árvízvédelemre vonatkozó első jogi rendelkezések is megjelentek. Fontos megemlíteni még a Werbőczi Tripartitumot is, mely a magyar szokásjogok gyűjteménye volt. Itt kerültek rögzítésre legelőször a vizekkel kapcsolatos legrégebbi jogelvek. Számos előírás szólt a vízhasználatokról. A vízfolyások rendelkezésének szabályaival kapcsolatban is születtek már a középkorban vízjogi rendelkezések – elsősorban a Maros, a Tisza és a Szamos tekintetében. Összességében nézve, egészen a XVIII. század végéig a magyar vízjogi fejlődést az ország földrajzi és vízrajzi viszonyaihoz való alkalmazkodás jellemezte. Az iparosodás korszakában a technológiai fejlesztések a vízgazdálkodást is utolérték. Kiépítésre kerültek az első ivóvíz- és csatornarendszerek hazánkban is. (Az 1790-es éveket megelőző időkből csatornák ugyanis alig maradtak fenn, az első víz – és csatornaművek 1790-1830 között kerültek megépítésre.) A vízgazdálkodásban történt változások pedig hatással voltak a hazai vízjogi rendszerre is. A vízművek vízszolgáltatását, a víz használatát, az elfogyasztott víz ellenértékének megtérítését már ekkoriban kormányhatóságilag jóváhagyott szabályrendeletek határozták meg. Rendelet mondta ki például, hogy a csatornák megépítési költségeit a város, valamint a köztelkek tulajdonosai viselték. A vízjogi rendelkezések a XIX. században tehát már a vízellátásra, csatornázásra, valamint a vizek védelmére vonatkozó előírásokat is tartalmaztak. A vizek tulajdoni viszonyait tekintetve pedig egyre dominánsabbak lettek a köztulajdoni jellegek: minden hajózható víz az állam közvagyona lett, magántulajdonnak pedig már csak a birtok területén összegyűlt és folyó vizek számítottak. A vizek köztulajdoni jellegét tovább erősítette: A vízjogról szóló 1885. évi XXIII. törvénycikk is, mely szabályozta a felszíni és felszín alatti vizek tulajdonjogát, meghatározva az állami tulajdon (közvizek) és a magántulajdon körébe (magánvizek) tartozó vizek, vízi létesítmények kategóriáit. Ez a törvény rendelkezett a vízmunkák elvégzéséről is, melyet hatósági engedélyhez kötöttek és a hatóság műszaki szakértőjeként pedig a kultúrmérnöki hivatalokat jelölték meg. Továbbá a törvény kimondta azt is, hogy vízfolyásokban történt változásokért, létrejött károkért a vízközművek tulajdonosai kötelesek kártérítést fizetni. A törvényben szabályozásra kerültek a vízi társulatok feladatai és működései is. A következő említésre méltó vízjogi szabályozási tevékenység a vizek mennyiségi védelmére vonatkozott elsősorban. Ez az 1913-as újabb szabályozás (az 1913. évi XVIII. törvénycikk) a vízjogról szóló alaptörvényt egészítette ki. A vizek tisztaságának érdekében is született több olyan jogszabály, melyek idevonatkozó rendelkezési már a közegészségügyi szempontokat is figyelembe vette. Ekkoriban az ivóvízellátásának jogi fejlődésére a legnagyobb hatást az Országos Ivóvíz ellátási Nagygyűlés

gyakorolta, mely célja az volt, hogy felhívja a közvélemény figyelmét egészséges ivóvízellátás megteremtésének fontosságára. (Az 1900-as éves első felében az ásott kutak háromnegyed részének a vize ugyanis még ártalmas volt az egészségre.) [1] [2]

A vízügyről szóló 1964. IV. törvény, mely a második vízügyi alaptörvény lett az 1885. évi XXIII. törvény után, még inkább az állam tulajdonviszonyát, annak felelősségvállalását, a korlátlan gondoskodási kötelezettségét és közvetlen beavatkozást jelentő végrehajtó-rendelkező tevékenységét erősítette. A törvény kimondta azt is, hogy vízdíjat kell fizetni „a vizek és vízlétesítmények használatáért", továbbá szennyvízbírság fizetésére kötelezte „a vizek fertőző vagy károsan szennyező üzemeket" Lényeges módosítás az első törvényhez képest az volt, hogy a feladatok már külön környezetvédelmi és külön vízügyi feladatokra tagozódtak szét. A vízügyi hatóságok feladatit és a vízügyi igazgatást az Országos Vízügyi Főigazgatóság irányította. A törvényben szerepet kapott már a vízminőség is. Tilos volt a vizeket fertőzni, azokba káros szennyeződéseket juttatni, továbbá minden olyan behatástól védeni kellett, ami azok fizikai, biológiai és kémiai tulajdonságát, minőségét és öntisztulási képességét hátrányosan megváltoztatta. [3]

Ez a vízügyi törvény sok beruházás létesülését eredményezte. Említésre méltó a két tiszai vízlépcső megépülése vagy a rengeteg vezetékes ivóvízhálózat és szennyvízelvezető csatorna létesülése.

A hazai vízjog történetében a következő említésre méltó törvény: az 1995. évi LVII. törvény a vízgazdálkodásról. A törvény megszületésére főleg a rendszerváltás miatt volt szükség, mely hatására a társadalomban és gazdaságban létrejött változások maguk után vonták a hazai jogszabályok, törvények felülvizsgálását és módosítását. A törvény hatálya többek között kiterjedt a „felszín alatti és a felszíni vizekre (a továbbiakban: vizek), a felszín alatti vizek természetes víztartó képződményeire, illetőleg a felszíni vizek medrére és partjára", „arra a létesítményre, amely a vizek lefolyási és áramlási viszonyait, mennyiségét, minőségét, medrét, partját vagy a felszín alatti vizek víztartó képződményeit befolyásolja vagy megváltoztathatja" [4], továbbá azokra a tevékenységekre, melyek az említett vizeket és létesítményeket befolyásolják, megváltoztatják. A törvény hatálya még kiterjedt a vizek hasznosíthatóságára, a vízkárok elleni védekezésre, védelemre, a vizek megismeréséhez, az állapotuk feltárásához szükséges mérésekre, adatgyűjtésekre, azok feldolgozására, a vizek állapotának az értékelésére, kutatására is és az eddig megemlített tevékenységet folytató természetes és jogi személyekre, gazdasági társaságaira. Az állam feladataként meghatározta a vízgazdálkodás országos koncepciójának a kialakítását, jóváhagyását, a nemzetközi együttműködésből adódó vízügyi feladatok ellátását és a vízkár-elhárítási tevékenység szabályozását, szervezését, irányítását, ellenőrzését, a helyi közfeladatokat meghaladó védekezését, továbbá az önkormányzatok feladatköreit is. A törvény a tulajdonviszonyokat is rendezte megfelelően, azaz az állam kizárólagos tulajdonba tartozó folyókról, patakokról és holtágakról, mellékágakról, azok medreiről, továbbá a vízi létesítményekről név szerinti felsorolást tett közzé. Törvényi szinten szabályozta már a vízi közművekkel végzett tevékenységeket is. Hatósági feladatként a vízügyi felügyeletet kötelezettségé tette, mely kiegészült a vízgazdálkodási bírság jogintézményével. Szabályozásra került a vizek kártételei elleni védelem is, és rögzítette a vízigény kielégítési és vízkorlátozási sorrendet. [4] [5]

A három fontos törvény a következő táblázatban kerül rövid összehasonlításra:

Év	*1885*	*1964*	*1995*
Cím	a vízjogról szóló XXIII.	a vízügyről szóló IV.	a vízgazdálkodásról szóló LVII.
§-ok száma	196	46	45
Tartalom fő jellemzői	– tulajdoni alapon mindent a társulat végez – kényszer alkalmazása (alakítás, csatolás, fizetés) – közérdek	– a vízügy az állam feladata – közérdek – vízügy a domináns	– állam, önkormányzatok, érdekeltek feladata tulajdoni alapon – nincs kényszer – vízügyi szakmai irányítás, koordináció
A védekezés irányítója	– miniszteri biztos	– kormánybiztos, kormánybizottság	– kormánybiztos, kormánybizottság
Finanszírozás	– érdekeltségi hozzájárulásból – állami támogatásból (1/3) – kötelezés a végrehajtásra	– a fejlesztés a fejlődéssel és az erőforrással arányos – biztonsági követelményszintű fenntartás	– a közérdek mértékéig az állam – érdekeltségi hozzájárulás – közcélú érdekeltségi hozzájárulás

1. táblázat. A három „vizes” törvény összehasonlítása
Forrás: Babák Krisztina: A magyar vízügyi törvények a kezdetektől napjainkig
http://geography.hu/mfk2004/mfk2004/phd_cikkek/babak_krisztina.pdf

A VÍZJOGBAN TÖRTÉNT JELENTŐSEBB VÁLTOZÁSOK 2000 UTÁN

A vízjogban történő újabb és jelentősebb változásokat aztán az uniós csatlakozásunk hívta életre. Az Európai Unióhoz történő csatlakozásunk előtti jogharmonizáció tette szükségessé többek között a vízgazdálkodásról szóló törvényünk módosítását is. A 2001. évi LXXI. törvény a vízgazdálkodásról szóló 1995. évi LVII. törvény módosításáról mind az állam, mind az önkormányzatok részére újabb feladatokat határozott meg. Állami feladat lett „a vízgazdálkodás országos koncepciójának, valamint ezen koncepció egyes részterületeit érintő nemzeti programok kialakítása és jóváhagyása” [5], továbbá ezeknek a megszervezésének a végrehajtása. A települési önkormányzatok feladatai is bővültek. Feladataik közé tartozik például:

- a helyi vízi közüzemi tevékenység fejlesztésére vonatkozó tervek kialakítása, végrehajtása
- helyi víziközművek működtetése, valamint a koncessziós pályázat kiírása, elbírálása, a koncessziós szerződés megkötése
- gondoskodás a települési közműves vízszolgáltatásra vonatkozó terv jóváhagyásáról, a vízfogyasztás rendjének a megállapításáról
- a vízgazdálkodással kapcsolatos önkormányzati szintű hatósági feladatok ellátása
- a természetes vizek fürdésre alkalmas partszakaszainak a kijelölése
- a helyi vízrendezés és vízkárelhárítás, és árvíz – és belvízelvezetés
- gondoskodás a települések lakott területein az ivóvízellátásról és a használt vizek szennyvízelvezető művel való összegyűjtéséről, tisztításáról, a tisztított szennyvíz elvezetéséről.
- hulladékgazdálkodással kapcsolatos feladatok (melyeket külön jogszabály ír elő) [5]

Víz Keretirányelv

2000. december 22-én lépett hatályba „A közösségi cselekvés kereteinek a meghatározásáról a vízpolitika területén” című 2000/60 EK Irányelv (röviden: VKI), ami az uniós vízpolitika legfőbb eszközévé vált. [2] Fontosnak tartom megemlíteni, hogy bár a vízzel kapcsolatos kerettervezési rendszer fontosságát az európai vízjog csak 2000-ben ismerte fel, addig hazánkban ez az elképzelés már törvényi szinten is megfogalmazódott az 1964-es vízügyi törvényben. Az 1964-es törvény 4. § kimondta, hogy „a vízgazdálkodási tervezés alapja az Országos Vízgazdálkodási Keretterv” [6]. Az új uniós vízpolitika azt a célt tűzte ki, hogy 2015-ig jó állapotba kell hozni minden olyan felszíni és felszín alatti vizet, amelyek esetén ez egyáltalán lehetséges és fenntarthatóvá kell tenni a jó állapotot. A VKI minden olyan emberi tevékenységre kiterjed, amely jelentős mértékben negatívan befolyásolhatja a vizek állapotát, akadályozva így a vizek jó állapotának elérését, megóvását. A vízgazdálkodást nem határon belül, hanem azon túlnyúlva a vízgyűjtő területenkénti megvalósulását segíti elő hozzájárulva a vízvédelem harmonizálásához és a vizek terhelésének csökkentéséhez. Az Irányelv által meghatározott feladatok végrehajtásáért minden tagország maga viseli a felelősséget. A legfontosabb feladatok a következők:

- állapotfelvétel (jelenlegi állapot),
- a célok meghatározása (az elérendő állapot),
- intézkedések meghatározása a célok eléréséhez.

Fontos részfeladatok a következők:

- Vízgyűjtő egységek meghatározása
- Nemzetközi vízgyűjtő egységekhez való besorolás
- A vizek jellemzőinek elemzése a vízgyűjtőkön:
- A felszíni víztípusok megállapítása
- Referencia-feltételek és mérőhelyek megállapítása
- A felszín alatti vizek leírása
- Az emberi tevékenységek hatásainak vizsgálata
- Jellemzési kritériumok kidolgozása
- Felügyeleti módok megállapítása
- A vizek állapotának értékelése
- Gazdasági elemzések elvégzése
- A költség-visszatérülés elvének átültetése
- Az intézkedési programok meghatározása [7]

A VKI jelentősége abból adódott, hogy egységes alapokra helyezte a felszíni és a felszín alatti vizek minőségi és mennyiségi védelmét, a pontszerű és a területi szennyező-forrásokkal szembeni fellépést. A vizek védelmét egységes, főleg ökológiai szempontok alapján hajtja végre. További célja a fenntartható vízhasználhatóság biztosítása, valamint a vízvédelmi – és a vízgazdálkodási politika összehangolása. Továbbá a gazdasági megfontolásokat figyelembe véve előírja a vízszolgáltatások költségeinek szektoronkénti megfelelő mértékű fedezését. Megfogalmazza, hogy a vízárak alakulásának elő kell segítenie a víztestek állapotának a javulását, valamint hosszútávon a maguknak a vízhasználatoknak a fenntarthatóságát. [2]

A VKI hatályba lépése számos jogi következménnyel és jogharmonizációval járt együtt hazánk számára. A VKI hazai jogrendbe való ültetése 2003-ban kezdődött meg és 2015-ig fog tartani. Előírja például a vizek jó állapotának eléréséhez vezető intézkedések vízgyűjtő szintű összehangolását. Magyarország számára ennek kiemelt fontossága van, mert hazánk egész területe a Duna vízgyűjtőjében fekszik, és a VKI szerint az egész Duna medencét kell vízgyűjtő területnek tekinteni. (A Duna egész vízgyűjtőjére vonatkozó tevékenységet a Duna Védelmi Egyezmény Nemzetközi Bizottsága – az angol rövidítés szerint ICPDR –

koordinálja.) A Víz Keretirányelv rendelkezéseit integrált módon, a vízgyűjtő-gazdálkodási tervezés eszközeivel kell végrehajtani az érdekeltek széleskörű bevonásával. Az EU tagországoknak 2009-re saját vízgyűjtő-gazdálkodási tervet kellett készíteni. [8]

AZ IVÓVÍZ MINŐSÉGÉNEK JELENLEGI SZABÁLYOZÁSA

201/2001. (X.25.) Korm. rendelet

Az ivóvíz az a víz, amit a köznyelv csapvíznek is hív. Hazánkban az ivóvíz minősége a manapság már a magyar és európai jogszabályok által szigorúan szabályozott és az illetékes hatóság által ellenőrzött stratégiai fontosságú közegészségügyi kérdés. Az EU csatlakozás előtt más területekhez hasonlóan az ivóvíz minőségi követelményrendszerének a területén is jelentős jogharmonizáció kezdődött el. Az Európai Unió először 1980-ban adott ki az ivóvíz minőségének a szabályozására vonatkozó direktívát, amit sok kritika ért a tagországok részéről. Ezt a direktívát 1998 novemberében módosították és a helyébe az Európai Tanács 98/83/EK irányelve (1998. november 3.) az emberi fogyasztásra szánt víz minőségéről direktíva lépett. Ennek a direktívának a figyelembevételével készült el hazánkban a 201/2001. (X.25.) Kormányrendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről. A Kormányrendeletet megelőzően hazánkban még nem volt olyan rendelet, amely konkrétan csak az ivóvizek minőségével foglalkozott volna, csak szabványok álltak rendelkezésre, melyek ezen Kormányrendelet hatálybalépésével hatályukat vesztették. Ezek a szabványok a következők voltak:

- - MSZ 450-1:1989 Ivóvízminősítés fizikai és kémiai vizsgálat alapján;
- - MSZ 450-2:1991 Ivóvízminősítés mikroszkópos biológiai vizsgálat alapján;
- - MSZ 450-3:1991 Ivóvízminősítés mikrobiológiai vizsgálat alapján. [9]

A vízminőség a víz fizikai, kémiai és biológiai tulajdonságainak az összessége. Alapvető követelmény az ivóvízzel kapcsolatban, hogy ne tartalmazzon az emberre ártalmas élő- és élettelen anyagokat, feleljen meg a fogyasztók esztétikai igényeinek, és biztosítsa az emberi élethez szükséges mikro- és makro elemek felvételét és a só utánpótlását is. Az ivóvíz ívásra, főzésre alkalmas, továbbá élelmiszer készítésére, előállítására, vagy egyéb háztartási célokra használják. A víz minőségének meghatározása szakszerű mintavételből, valamint helyszíni és laboratóriumi fizikai, kémiai biológiai és bakteriológiai vizsgálatokból tevődik össze. A 201/2001. (X.25.) Kormányrendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről írja elő például a mintavétel módját, a vizsgálat számát, fajtáját vagy a vizsgálati módszerekkel szemben támasztott követelményeket. A Kormányrendelet 1. számú melléklete a minősítésre vonatkozóan 6 db táblázatban tartalmazza a vízminőségi paraméterekkel és a rájuk vonatkozó határértékekkel és megjegyzésekkel kapcsolatos adatokat, követelményeket. A 2. számú melléklet tartalmazza az ellenőrzési követelményeket, vizsgálandó komponensek és az előírt mintavételi gyakoriságokat- a vizsgálatok kapcsán ugyanis megkülönböztetünk ellenőrző (azaz mindig vizsgált paraméterek) és részletes vizsgálatokat. A különböző mintavételi módszereket és laboratóriumi módszereket lehetséges kivitelezését még mindig, az előírt szabványok (Magyar Szabványügyi Testület által elfogadott szabványok) írják le. Az ivóvíz minősítése végül az előírt vizsgálatok együttes értékelése alapján történik. Az előírt mintavételeket és vizsgálatokat a Fővárosi Vízművel és a regionális vízművek, illetve az ÁNTSZ országos, azaz az Országos Tisztiorvosi Hivatala (OTH) és regionális szervei és az Országos Környezetegészségügyi Intézet (OKI) végzi. Továbbá még vannak vízvizsgáló laboratóriumok. (A feltétel, hogy miden laboratórium rendelkezzen a Nemzeti Akkreditációs Testület által, az adott vizsgálatok elvégzéséhez jogosult engedéllyel, akkreditációval.) Minden üzemeltetőnek ugyanis gondoskodnia kell arról, hogy az ivóvíz minőségét ellenőriztesse akkreditációval rendelkező laboratóriummal.A rendelet kitér az ivóvíz

előállítása - beszerzése, kezelése, tárolása - és elosztása során használt vízkezelési technológiák és anyagok, szerkezei elemek okozta szennyeződés megakadályozása érdekében folytatott laboratóriumi vizsgálatokra is. Az idevonatkozó vizsgálati módszerek nagymértékben megegyeznek az ivóvíz (hálózati víz) minőségének ellenőrzésére szolgáló vizsgálatokkal. Megjegyzendő, hogy az ásványvizekre, termálvizekre és fürdővizekre ez a kormányrendelet nem vonatkozik. [10]

A vízvédelem ügyeit hazánkban a Környezetvédelmi és Területfejlesztési Minisztérium irányítja, elsőfokú hatósági szervek a vízgyűjtő területi elv alapján szervezett vízügyi igazgatóságok. A katasztrófa jelegű szennyezések eltávolítására - azaz rendkívüli események esetén – az adott illetékes népegészségügyi szerv a túllépés okát kivizsgálja, szükséges javító intézkedéseket megteszi és a szükséges technológiai védekezési módszereket dolgozzák ki. [11]

65/2009. (III. 31.) Korm. rendelet

A 201/2001. (X.25.) Kormányrendeletet aztán felváltotta a jelenleg is hatályban lévő 65/2009. (III. 31.) Korm. rendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről szóló 201/2001. (X. 25.) Korm. rendelet módosításáról. A módosított rendelet két lényeges új eleme: új településlistát tartalmaz, amely a 201/2001. (X.25.) kormányrendelet 6. sz. mellékletének további módosítását jelenti, továbbá előírja az ún. vízbiztonsági terv készítését. A vízbiztonsági tervre vonatkozóan a rendelet kimondja, hogy minden olyan vízellátó rendszereknek, mely 1000 m3/nap-nál nagyobb kapacitású vagy 5000 főt meghaladó ellátó, ivóvízbiztonsági tervet kell készítenie. Ez a vízellátó rendszer vízbiztonsági – irányítási rendszerét kell, hogy tartalmazza. A tervet az OTH hagy jóvá közegészségügyi szempontból. „A vízszolgáltatónak az ivóvízbiztonsági terv közegészségügyi felülvizsgálatát négyévente az OTH-nál kell kezdeményeznie.” [12] A terv jóváhagyásáról szóló határozatot pedig az illetékes környezetvédelmi és természetvédelmi és vízügyi felügyelőséghez is el kell juttatni.

A lakosság egészséges ivóvízzel való ellátása - a 98/83/EK irányelv és a hatályos Kormány rendeletben rögzített határértékek, illetve az OKI (Országos Környezetegészségügyi Intézet) szakvéleménye alapján - egyedi, illetve térségi ivóvízminőség-javító projektek keretében kezd megvalósulásra jutni. A Környezet és Energia Operatív Program KEOP 1.3. jelű kétfordulós konstrukciója keretében lehetőség adódik az ivóvíz minőség pályázati úton elnyerhető támogatással történő javítására. Magyarország számos településén ugyanis az ivóvíz minősége sajnos nem felel meg az európai uniós és az ezzel összhangban lévő hazai előírásoknak. Kiemelt fontosságú ivóvízminőségi jellemzők határértékeinek teljesítésére a Csatlakozási Szerződés határidőket is megállapított. A szolgáltatott ivóvíz minősége szempontjából problémás települések eloszlása nem egyenletes az ország területén. Magyarország egyes térségeiben nagy számban és nagy sűrűséggel érintettek a települések. Koncentráltan az Észak-alföldi, a Dél-alföldi, továbbá az Észak-magyarországi és a Dél-dunántúli Régiókban találhatóak olyan települések, amelyek ivóvize nem felel meg a 98/83/EK irányelv vízminőségi határértékeinek. Szórtan minden régióban találhatók nem megfelelő minőségű vizet szolgáltató vízművek. A Dél-Alföldön és Észak-Alföldön már jelentős lépések történtek az EU és a hazai előírások teljesítését szolgáló beruházások előkészítésére. A 1067/2005. (VI.30.) Korm. határozat alapján folyik az Észak- és Dél-alföldi Régiók Ivóvízminőség-javítási Programjainak előkészítése. A megvalósítás fázisára a két alföldi régiós program kisebb projektekre bontva valósulhat meg. A megfelelő ivóvíz minőség elérését a pályázat segíti, melyek keretében nyújtható támogatás a közműves vízellátás keretében szolgáltatott ivóvíz minőségének javítására, az előírt vízminőség biztosítására irányuló fejlesztések előkészítését, illetve megvalósítását segíti. [13]

A 65/2009. Korm. rendelet további lényeges eltérése a 201/20001. Korm. rendelethez képest, hogy a hatósági jogkör nemcsak már az ÁNTSZ-re és annak illetékes szerveire terjed ki, hanem a rendelet figyelembe veszi az ivóvíz élelmiszerek előállítása során történő felhasználását is, és ennek következtében hatósági jogkörrel ruházza fel az ivóvizek minőségi ellenőrzése kapcsán az „MgSzH”-t, azaz a Mezőgazdasági Szakigazgatási Hivatalt. Az üzemeltető által beküldött adatok összesítése, értékelése és az idevonatkozó jelentések elkészítése is feladata már az MgSzH-nak. A rendelet továbbá foglalkozik a házi vízelosztó rendszerekkel is az ivóvíz minősítése kapcsán. Az ÁNTSZ illetékes intézete, illetve az MgSzH köteles tájékoztatni a házi vízelosztó rendszer tulajdonosait és a fogyasztókat az egészségügyi kockázatok miatt az általuk tehető további intézkedésekről és beavatkozási módokról. Az üzemeltetőnek, illetve az élelmiszer-vállalkozásnak kötelessége a vizsgálat költségeit megtéríteni az illetékes hatóságnak jogellenes viselkedés és határérték-túllépés esetén.

A határérték szigorítások elsősorban a kémiai paramétereket érintik. Még a 201/2001. Korm. rendelet bizonyos anyagokra vonatkozó határértékeket csak az Európai Unióhoz való csatlakozásunkat követően tette kötelezővé, azaz volt még némi türelmi idő, ami természetesen már az újabb rendeletben érvényét vesztette és a határértékek betartása kötelező lett. Ezek a következő anyagok: antimon, bromát, 1,2-diklór-etán, peszticidek, összes peszticid, ólom [12]. A 201/2001. Korm. rendelet 2. számú mellékletében feltűntetett ellenőrző vizsgálatokra vonatkozó táblázatban is jól megfigyelhető a szigorítás a kémiai paraméterek vonatkozásában. Több vizsgálati paraméter lett előírva ugyanis az I. oszlopba tartozó mindig vizsgálni szükséges vízminőségi jellemzőkhöz. Ez a pH és a zavarosság mérésével bővült, míg a nagyon ritkán és a megjegyzésekben leírt feltételek bekövetkezte során szükséges vizsgálatok közül a klorit, a kötött aktív klór és a szabad aktív klór vizsgálatai pedig átkerültek a II. oszlopba, azaz - a megjegyzésekben leírt feltételektől függően vizsgálva- kategóriába.

Az új településlista pedig a hatályát vesztett rendelet 6. számú mellékletének egy tovább bővített, módosított változata. Szigorítások itt elsősorban a vas, mangán, arzén, bór és ammónium ion tartalomban leginkább a szembetűnök országos szinten.

A rendelet módosítására - meglátásom szerint - az elkövetkezendő tíz éven belül szükség lehet. Ezt avval indokolnám, hogy környezetük, életterünk és így a vízi ökoszisztémáink is egyre szennyezettebbé válik. Szükség lesz majd a már meglévő határértékek további szigorítására. Az olyan paraméterek vonatkozásában, melyekre jelen rendelet nem tartalmaz számszerű, konkrét határértéket, vagy a számérték helyett csak megjegyzésben és/vagy bizonyos estekben számszerűsítenek, elképzelhetőnek találom, hogy konkrét értéket fognak ezekre is megállapítani. Példának okáért a TOC, azaz a teljes széntartalom paramétert említeném, mely az indikátor vízminőségi jellemzők közt szerepel és a határérték rublikájában csak az szerepel, hogy: „Nincs szokatlan változás” és hozzá egy megjegyzés. A TOC értékét még csak a szerkezeti anyagok vizsgálatánál állapították meg 2 mg/l értékben. A mérések során viszont egyértelműen pontos számszerű értékeket kapunk, nem csak a szerkezeti anyagokat vizsgálva. Továbbá ez olyan vizsgálati paraméter, ami még nem olyan elterjedt hazánkban. Fontosságát viszont nagyon sok szakember látja és tapasztalja és egyre több vizsgáló laboratóriumban válik napi mérési paraméterré mind az ivóvizek, mind a szennyvizek vonatkozásában. Az evvel foglalkozó szakemberek már rengeteg olyan számszerű eredménnyel rendelkeznek, melyekből lehetőség nyílik majd jogi szinten is megállapítani a határértékeket.

Figyelembe kell venni azt a tényt is, hogy a tudomány előrehaladtával egyre több paramétert lesznek képesek a szakemberek bevizsgálni, vagy a meglévő módszereket

egyszerűbbé tenni, melyek esetlegesen újabb paraméterek feltűntetését teszik lehetővé törvényi szinten is.

Az egészségügyi kockázatok tekintetében nem kizárt az a lehetőség sem, hogy az ellenőrző vizsgálatok számát növelik újabb paraméterek bevizsgálásával és teszik jogilag kötelezővé.

ZÁRSZÓ

Mérnöki munkám során napi szinten vizsgálom továbbá szakvéleményezem a vízminták eredményeit. Az ivóvizes rendeletek, jogszabályok használata és betartása természetesen munkám részét képezik. A vízminták eredményközlései és kiadásai során pont a rendeletekben megadott határértékek figyelembevételével kell a különféle szakvéleményeket megírni és kiadni. Ebben az esettanulmányban tehát a munkám miatt vállalkoztam arra, hogy górcső alá vegyem a régebbi és a jelenlegi vízjogi rendeleteket, ezen belül is az ivóvíz minősítéssel foglalkozókat. A témával kapcsolatos kutatómunkám során azonban egyre inkább szembesültem azzal a ténnyel, hogy a vízjoggal kapcsolatos rendeletek, törvények olyan nagy mennyisége halmozódott fel már az ókor óta, hogy ezek mindegyikét taglalni, elemezni, lehetetlen vállalkozás egy esettanulmány erejéig. A történelmi áttekintésük során törekedtem a legfontosabbakat kiemelni. A történelem előrehaladásával egyre több olyan rendelet, jogszabály született, melyek a vízzel kapcsolatban egyre inkább a víz különböző részterületeire tértek ki. Vannak törvények, rendeletek például, melyek a vízgazdálkodásával, vagy a víz felhasználhatóságával foglalkoznak, vagy külön rendelet vonatkozik a felszíni vagy a felszínalatti vizek védelmére is. Az ivóvízzel kapcsolatos rendeletek áttekintését azért láttam fontosnak és emeltem ki külön, mert az idevonatkozó rendeletek viszonylag elég későn születtek meg, pedig az ivóvizet az ember naponta fogyasztja és használja, így annak minőségét biztosítani kell jogi szinten is.

Elmondható, hogy a vízjog szabályozását illetően a ma már rendelkezésünkre álló rengeteg magyar jogszabály összhangban van az európai jogszabályokkal. A hazai törvényi előírások jól illeszkednek a közösségi jogrendszerbe. Úgy gondolom, hogy a jelenleg hatályos „vizes” jogszabályok, rendeletek kellőképpen használhatóak a gyakorlatban, a különböző vizekkel foglalkozó szakemberek megfelelően tudják hasznosítani a mindennapi munkájuk során. Bár elképzelhetőnek tartom a jövőben, hogy némely esetben bizonyos rendeletek módosítására lehet szükség, melyekhez már biztosított a megfelelő jogi háttér. Szakmai szempontból nézve, a nehézséget jelenleg inkább ezeknek a jogszabályoknak a betartása jelenti, hiszen az Európai Unióhoz való csatlakozásunk óta sok olyan vízben lévő káros anyagra vonatkozó határértékek szigorodtak, melyek betartása határidőhöz kötött. Feladatok tehát vannak, melyek elsősorban a szakemberekre várnak, melyek teljesítéséhez már erős alapok állnak a rendelkezésre.

Felhasznált irodalom

[1] A vízjog története, kialakulása és fejlődése. Szervezeti felépítés http://www.epito.bme.hu/vcst/oktatas/feltoltesek/BMEEOVKAI02/c-a_vizjog_tortenete_kialakulasa.pdf, (letöltve: 2011.11.06.)

[2] Báthori Mónika: A vízgazdálkodási törvény változása kezdetektől napjainkig, valamint a vízgazdálkodás jogi harmonizációja, KDVKÖVIZIG

[3] 1964. évi IV. törvény a vízügyről http://www.1000ev.hu/index.php?a=3&param=8450, (letöltve: 2011.11.11.)

[4] 1995. évi LVII. törvény a vízgazdálkodásról http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99500057.TV, (letöltve: 2011.11.11.)

[5] Babák Krisztina: A magyar vízügyi törvények a kezdetektől napjainkig http://geography.hu/mfk2004/mfk2004/phd_cikkek/babak_krisztina.pdf, (letöltve: 2011.11.10.)

[6] 2001. évi LXXI. törvény a vízgazdálkodásról szóló 1995. évi LVII. törvény módosításáról http://www.euvki.hu/content/docs/2001_lxxi_es_1995_lvii_tv.pdf, (letöltve: 2011.11.11.)

[7] EU Víz Keretirányelv http://www.euvki.hu/, (letöltve: 2011.11.09.)

[8] Székely Erzsébet - Piliszky Zsuzsanna: Víz, vízvédelem című távképzési anyag, Nők a Balatonért egyesület, 2009.

[9] For Aqua – Értünk: Ivóvíz szabvány http://www.foraqua.hu/ivoviz-szabvany.html, (letöltve: 2011.11.11.)

[10] 201/2001. (X.25.) Kormányrendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0100201.KOR, (letöltve: 2011.04.11.)

[11] Dr. Halász László – Földi László: Környezetvédelem – Környezetbiztonság: 5. Vízminőség – védelem. Egyetemi jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Vegyi és környezetbiztonsági tanszék, 2000, 95-111.p.

[12] 65/2009. (III. 31.) Korm. Rendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről szóló 201/2001. (X. 25.) Korm. rendelet módosításáról http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=A0900065.KOR, (letöltve: 2011.11.20.)

[13] Tájékoztató a KEOP-1.3.0 Pályázathoz szükséges OKI szakvéleményről http://www.antsz.hu/portal/down/kulso/kozegeszsegugy/kornyezeteu/KEOP-OKI_20080207.pdf, (letöltve: 2011.11.24.)

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Hornyacsek Júlia
hornyacsek.julia@uni-nke.hu

SYSTEMATIC APPROACH OF THE PREPARATION OF POPULATION IN THE FRAME OF A CHANGING DEFENCE SCHEME

Absztrakt / Abstract

Az elmúlt időszakban egyre nyilvánvalóbbá válik, hogy a megszaporodó, jellegükben átalakuló és intenzitásukban mindinkább romboló katasztrófa-helyzetek hatékony kezelése és a következmények felszámolása összetett és bonyolult folyamat. E folyamatban a hivatásos mentőerőkre hárul a munka legnagyobb része, de a jövőben szerepet kell vállalnia benne a településeknek, és az ott élő állampolgároknak és a civil szervezeteknek is. A szakemberek egyöntetű véleménye, hogy sok katasztrófa eleve megelőzhető lenne, ha a lakosság rendelkezne a megelőzéssel kapcsolatos legfontosabb ismeretekkel. A bekövetkezett katasztrófák kezelése is hatékonyabb ott, ahol az állampolgárok megfelelő veszélyhelyzeti, önmentési felkészítést kapnak. Felmerül a kérdés, hogyan, mi módon lehetne a felkészítési mutatókat javítani, milyen célcsoportokat lenne célszerű kialakítani a felkészítésre, és azt milyen módszerekkel lehetne végrehajtani.

It has become more and more obvious that recently there have been a growing number of catastrophy situations, their nature has changed and they have become more and more destroying regarding their intensity; managing them and eliminating their consequences is a complex task. Nowadays, the majority of it is done by regular rescue forces, but in the future settlements and citizens, and also civil organizations are expected to be involved in it. Experts unanimously claim that a lot of catastrophes could be prevented if citizens could master the major concepts of prevention. Also, managing of existing emergencies is more efficient, if citizens have been prepared thoroughly to tackle such situations and have been trained to self-rescue. It is a debatable question, how to raise the efficiency of preparation, what target groups to form for preparation, and what methodology to use to reach this goal.

Kulcsszavak/keywords: *katasztrófavédelmi felkészítés, célcsoport, felkészítési tartalmak, felkészítési módszerek ~ preparation for Disaster Management, target group, preparation contents, preparation methodology*

INTRODUCTION

"Catastrophes are like ghosts closed in a bottle: they are just waiting for an irresponsible or ignorant person to get the cork out." we claim quite often, and seemingly, nowadays it proves to be true, as not only the number of catastrophes has raised, but also their character has changed. Consequently, the defence system should follow these changes in order to be able to protect the population and their assets; rescue operations and methods should be altered, the most suitable equipment and methods should be deployed.

"Are we aware of the basic knowledge which enables us to save our and other's lives while the regular rescue team is on the way to arrive?"[1]

The defence sphere could be well-prepared, however, all efforts could fail, if the population is not trained to realize the dangers around them and to react on them, and also for avoiding them, or, in case of a catastrophe, to follow a proper behaviour. The flood in Borsod in 2010, the Kolontár catastrophe, and also extreme irregularities in weather, occurring day by day, or any other catastrophe situations has shown us that the knowledge and skills of how to survive are not at all innate, and this way we are exposed to nature forces and civilization. European countries, including Hungary undertake the responsibility to spread the knowledge, namely, to prepare the population for emergency situations.

During the Cold War, preparatory operations took place with an aim for protecting against nuclear war, in an exaggerated rate and measure, but the whole country, including all production areas were covered.

After the years of the democratic transformation the social and economic changes took place very fast, and priorities got passed on from the previous tasks to new areas. Thus, defence and preparations of the population were not at all an issue of major inters, on the contrary, the concepts, framework and methods of preparations were not even our lined neither from a strategic point of view nor from a tactic one.

At operational level, organizations and bodies, either official or civil and humanitarian ones, conducted individual preparation practices. Ordinarily, it was not synchronized at a national level.

Nowadays, there is a raising demand for a synchronized, centralized preparation system that would overlap organizations and ministries. Meanwhile, however, until it comes alive, the responsibility and duty will fall onto official defence organizations, which means that themselves, along with civil bodies and organizations around them, should transfer this special knowledge, through coordinating the preparation activities. Each preparation force means the concept of preparations in a little bit different way, and it sometimes results in duplication, and in other cases in alternative methods in practice.

In the present study, further on, I challenge proposing a concept for the preparations for a forecoming catastrophe, for its requirements, the target groups to be prepared and for its content and methodology.

[1] Júlia Hornyacsek-Veres: Theoretical and Practical Questions of Preparing the Population for Emergencies, Vol. 1., ZMNE, Budapest, 2005. p.3.

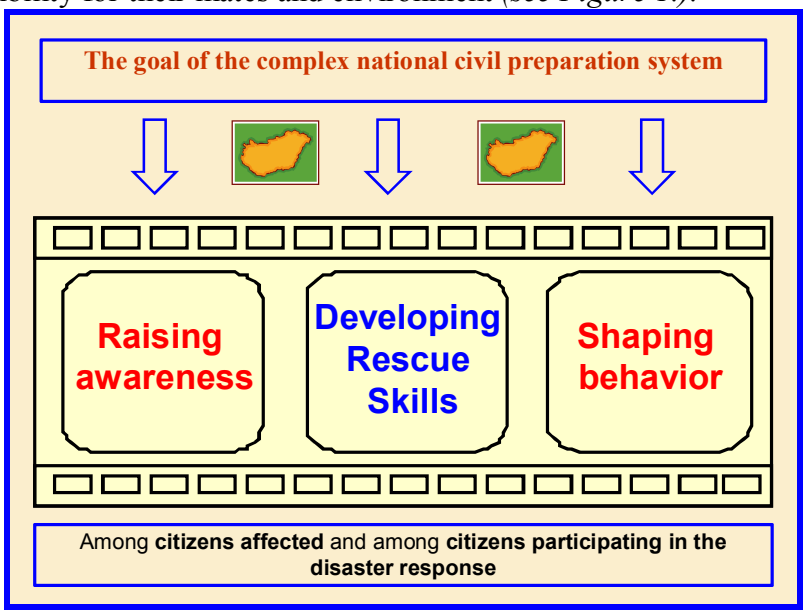
CONCEPT, AIM AND PURPOSE OF THE PREPARATION OF THE POPULATION FOR A FORECOMING CATASTROPHE

The preparation of the population is a broad concept, it covers everything which is transferred towards them by the various elements of the defence sphere, for their protection. To be able to define the methods of *catastrophe-related preparation*, primarily its concept should be defined, as there is no unified interpretation for it in this area.[2]

Here I propose a concept for the preparation of the population for a forecoming catastrophe as follows:

Preparation of the population for a forecoming catastrophe is *a system of activities***,** in which the population is *preparing* to tackle danger situations either above or below a catastrophe threshold and skills are *building up,* with the help of which citizens can successfully rescue themselves, their mates and assets. *Furthermore*, the defence knowledge and rescuing skills in eliminating catastrophes are *establishing* in the civilian population.[3]

The *basic aim* of the preparation of the population is to *familiarize* danger situations with a broad range of citizens, suffering from the harmful effects of an emergency, or being threatened by one, and also familiarize these hazardous situations with the civilian population being involved in the rescue operations, the behaviour and action patterns to follow, and the ways of rescuing themselves or others, and their assets. It is also important to make the population *realize* that they can also cause emergencies. Furthermore, there is an *indirect aim* to establish the security culture of citizens, and to enhance their sense of social responsibility, e.g. the responsibility for their mates and environment *(see Figure 1.)*.



1. figure. Direct and indirect aims of the preparations
Prepared by Dr. Júlia Hornyacsek, 2010.

Population means "the total number of the inhabitants of a given area or settlement".[4] For further investigations I have to define the concept of population in the frame of the

[2] Formerly, the preparation of the population belonged to the sphere of civil defence, and BM Decree 13/1198 was provisional about it. Along with changes in the provisions of law this topic has been approached in a different way.
[3] Wording of the author
[4] Szilvia Csábi, 2003.

preparations. Regarding the above, it is obvious that here the concept of population means something different from what commonsense suggests.

From the point of view of preparations the concept *population* is the total number of Hungarian and non-Hungarian citizens living in Hungary, who are exposed to dangerous effects and who need to be prepared for emergencies and for actions to be taken in these situations. Citizens can be ranked in a lot of ways according to their gender, age, occupation, field of interest, level of danger, and their preparation should be adjusted accordingly.

Preparation of the population, as a system:

Summarizing the results of the research done in this field, one can say that it is a complex system of actions, which has also subsystems. These are as follows:

- subjects of preparations;
- providers of preparations;
- preparation material, its content and layout;
- periods of preparations;
- preparation tasks;
- preparation methods;
- conditions of preparations.

Legal background of the preparations

Different defence organizations transfer different information towards the population, as each of them executes the preparation upon their own special field. Their activities are defined by the provisions of law. The frames of the present study do not make it possible to discuss all of them, so here I present the two provisions covering *civil defence* and *Disaster Management*.

There are several provisions of law concerning the preparations, but this activity is only specified *in BM Case "13/1998.(III.6.) About the requirements of civil defence preparations"*. The case includes the preparations by civil defence organizations formed upon obligation and participating in eliminating catastrophes, the requirements on civil defence exercises, the key concepts of organizing a civil defence exercise, the knowledge to be transferred in a civil defence basic training, and the knowledge of civil defence professional training. It also contains the civil defence preparation of a wider range of the *population* and of the employees of civil organizations, their requirements and contents.

Plants producing or processing hazardous materials are ranked as high or low threshold ones, depending on the amount of dangerous materials processed. "A given plant could mean a risk for the population living in its sphere of operation, thus people have the right to get to know the potential hazardous effects, the methods of tackling them, and the behaviour patterns to follow in case of a serious accident." [5]A building permit can be issued only by the Disaster Management permit of the central organization of a regular Disaster Management body. Both a low and a high threshold plant make a plant-security analysis and send it to the authorities.[6] The authorities announce the mayors of the hazardous settlements on conducting the permission procedure for a new plant producing or processing hazardous materials, through sending them the security analysis.[7]"The concept of external defence plan contains

[5] Dr. Imre Varga, 2005.
[6] Law 2011. CXXVIII. on Disaster Management and the Modification of Related Laws, Chapter
[7] 7. ib. id.

the set of the defensive methods and measures to be taken for the protection of the population".[8]

The mayor makes an external defensive plan for the protection of the population in the area. Within a given time from the recept of the security report, he announces it publicly, together with the security analysis, e.g. he informs the population on the dangers in the settlement and on the actions to be taken in case of an accident. He is made certain on the applicability of the plan in defence exercises. For this, those who live in the area should be prepared.

Since the Cold War is over, the threat for a global nuclear war has been reduced to minimum, but the world has remained the same instable. The number of local conflicts, asymmetric tools deployed by non-state armed forces, terrorists, extremist groups have grown considerably. Chemical, biological, radiological and nuclear (CBRN) weapons and carrier systems keep spreading and have been developed globally. Nowadays, nuclear terrorism means a significant danger beside power plant accidents.[9]

Government Decree 165/2003(X.18) on the order of informing the population in case of a nuclear and radiological emergency claims that a Population Information Plan should be prepared on national, sectoral and county levels.

"The Population Information Plan is prepared in the interest of the population and contains all the concepts, methods and tools of supplying information upon which informing will be successful. Its aim is to win the citizens' confidence and also build on it, to establish efficient information supply in the period of prevention, and to protect the health of the citizens in case of an emergency."[10] The Plan should contain the fundamentals of radioactivity, its effects on humans and the environment, different types of nuclear and radiological emergencies and their consequences, precautions for the protection of the population, and tasks of the citizens in case of emergency.[11]

REQUIREMENTS ON THE PREPARATIONS

In the frame of the Disaster Management system the tasks aimed at the protection of the population have an important role (see Figure 2.).

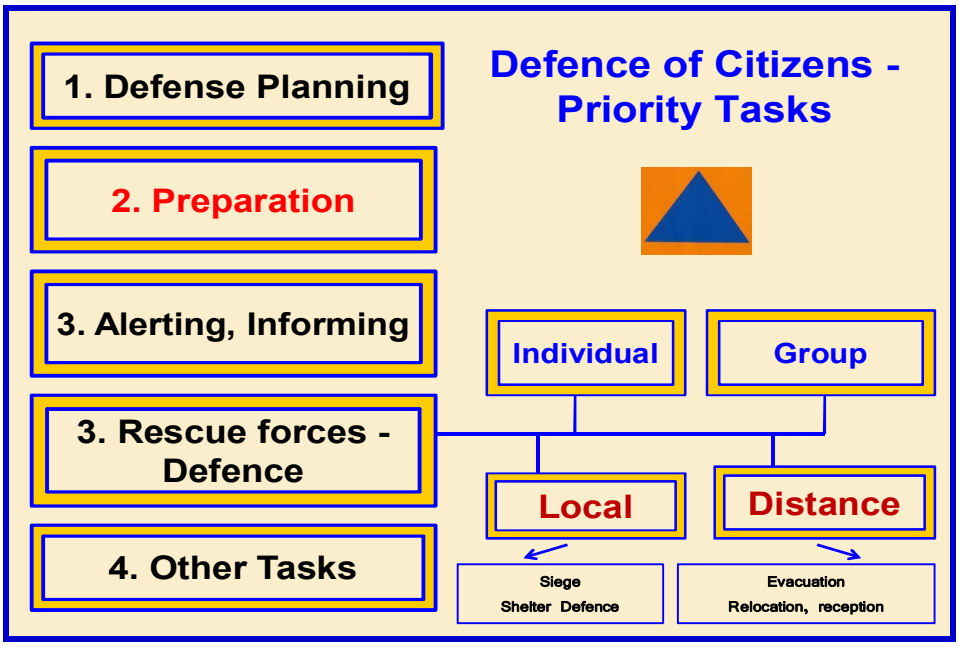
Executing preparation tasks is inevitable for the protection of the population. European countries manage this issue on a national level, but they also consider EU, NATO and UNO recommendations and action plans, and they form a new preparation framework and methods in the spirit of new challenges. Consequently, Disaster Management preparations differ for country to country so they meet different requirements. I analysed the Hungarian practice and collected these requirements.

[8] Gov. Decree 2/2001(I.17.) About Protection against Major Accidents Hazards Involving Dangerous Substances 16§ (2) and modifications

[9] Rezső Pellérdi, 2007.

[10] Gov. Decree 165/2003. (X.18.) About the Order of Informing the Population in Case of Nuclear or Radiological Emergency (Appendix 1., P.1)

[11] The discussed provisions of law are before a modification, supposedly, however, there also will be provisions of law after the modifications, which would claim the concepts, framework and contents regarding preparations.



2. figure. Prioritized tasks for the protection of the population
Prepared by the author

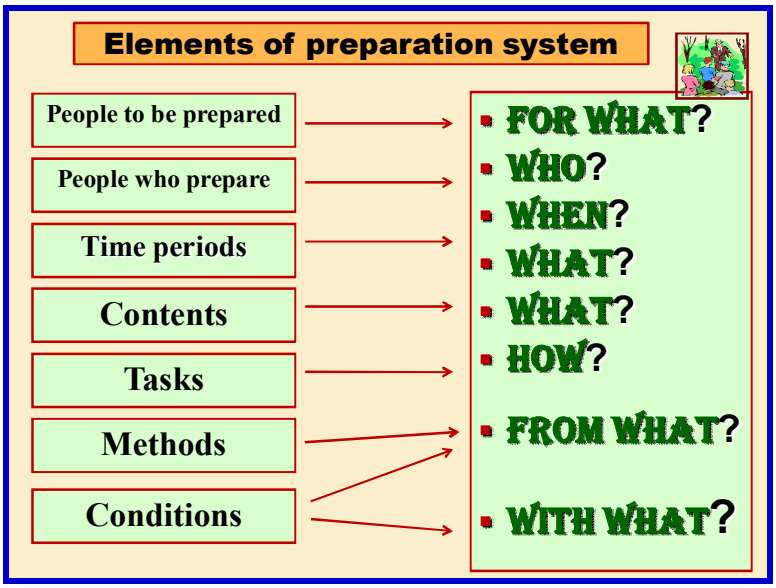
Requirements on the preparation of the population:

- The new system of the preparations should answer to new challenges, the emerging new and also the conventional emergencies, it should mix the useful elements of previous population-preparation systems with the new ones.
- The contents of the preparations should meet the country's level of insecurity and also the local conditions. It should detail emergency information on civil defence, fire-fighting, Disaster Management from the point of view of emergencies below a given catastrophe threshold.
- It cannot infract the existing provisional background or the opportunities, framework or principles offered by the modified rules of law.
- The preparation for facing catastrophes is expected to fit into the organizational structure, directing system, operational features, power and equipment capacity of Hungary's Disaster Management scheme.
- It should create and also take advantage of the concept of volunteering. Its methods should meet the needs of the target groups to be prepared, the local conditions and the affordable financial resources.
- The rule of "not anybody for anything" should apply, i.e. each target group should be prepared for the hazards in which they can possibly be involved, and to such measure and rate, which is necessary and also satisfying (possibly following a module scheme).
- It should meet the requirements of the Modern Era regarding its tools: it cannot be confined to giving lectures and handing out leaflets, but it should also include new preparational methods.
- It should save expenses, and it should comply with the preparation activity of the other components of the defence sphere.

THE COMPLEX SYSTEM OF PREPARATION

"The trouble that we are aware of and that we prepare for in advance can be overcome, even if with difficulties." -
Lívius -

The preparation procedure could comply with the above requirements, if it is regarded and operated as a complex system, which has various subsystems or elements. I summarized these in Figure 3. and I analyze them in detail in the present subsection.



3. figure. Elements (subsystems) of the preparation system
Prepared by the author

The groups of subjects: the target groups

It became obvious from the mistaken preparation practice of the 80's that it is impossible to prepare the population of the whole country at the same time, therefore a region can operate successfully, if the target groups of the population are well defined and the level, the course, the priorities of their preparation are set. But what is defined as a target group?

The target group of preparations: a segment of the population to which the given preparation activity refers to and whose size, composition, directions would define the contents, methods and tools of preparations. Upon analyzing the preparations throughout the country and also evaluating the observations of my own preparation exercise I grouped the population on the basis of their *role in the social division of labour* and of their *involvement or tasks* in possibly occurring catastrophes, in this way I assigned target groups as follows:

I separated three major target groups *upon their social division of labour*, and I also assigned further subgroups, whose preparations should be conveyed in different forms and contents.

I rank the following population as "employees":

- subordinates of a civil defence organization ;
- non-subordinates of a civil defence organization, but being prepared at their place of work
- non-subordinates of a civil defence organization, and not being prepared at their place of work;
- those getting in relation with an emergency while performing their duties;
- subordinates of ministries, state management and their bodies.

I rank the following population as "unemployed":

- students;
- pensioners, housewives;
- unemployed citizens.

I rank the following population as others:

- tourists;
- migrant workers;
- employees of foreign agencies;
- inhabitants of law-enforcement agencies;
- the handicapped, the sick, orphans, etc., trated in institutions.

The following target groups are advisable to form upon *their involvement in catastrophes and their tasks*:

- top managers and subordinates of ministries, law and order protection bodies, organizations of national authorities;
- area and local managers of defence directorates, leaders of local governments (mayors, town- clerks), and further groups that would encounter catastrophes upon carrying out their duties;
- leaders of voluntary, charity and civil organizations;
- leaders and subordinates of civil-defence organizations;
- a broader range of population, who are endangered by catastrophes, but who are not prepared in any other way as they do not belong to any of the above mentioned groups. Naturally, this group can be ranked according to various points of views (age, education, field of interest, state of health, etc.) so preparations could vary.

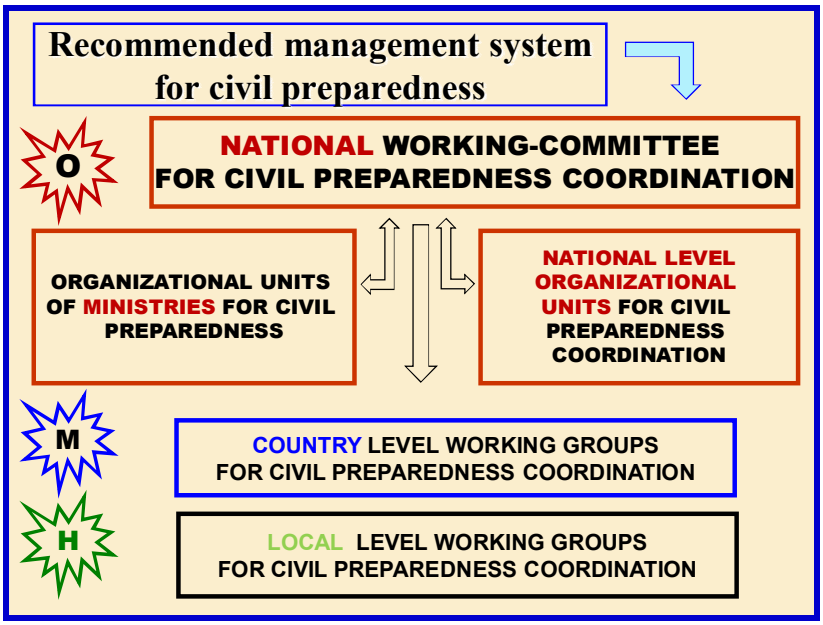
The groups of providers

The task of preparation providers is to convey knowledge towards subjects. The activity of preparation providers fall primarily on regular authorities in Hungary - unlike a number of European countries -, but more and more civil organizations and institutions join this procedure, thus a so called "mixed" preparation scheme is beginning to take shape in Hungary, in which volunteers, alliances, etc. participate in the preparations of the population beside the regular authorities of Disaster Management. The preparation activity is coordinated by the mayors and the leaders of defence organizations, in which they receive a major professional support from the county directorates of Disaster Management, and, at local level, from the office managers of civil defence agencies. At this point, the scheme is becoming "mixed", as volunteers and mayor-supporters, who are naturally civilian population, but undertook to be trained as providers, can join this activity.

There is no separate national, county or local organizations for coordinating the preparation activity: the defence system operates through the coordination and orientation of the defence organizations of the given level. I have analyzed the practice followed in the

neighbouring countries and the possibilities of the national preparations scheme, I have also conducted an efficiency analysis concerning orientation, and I have concluded that catastrophe-related preparations could be more efficient in the future if all knowledge and power of preparations would be concentrated; this is now represented by partner organizations parallely (see Figure 4.).

It would be advisable to set up a national coordination committee, and also coordination teams at county and local levels, which would define the concepts, framework, tasks and people in charge of the given preparations level, the distribution of affordable resources, the preparation of providers, etc.



4. figure. Elements (subsystems) of the preparations scheme
Prepared by the author

Preparation material, its contents and layout

Preparation content depends on the level of emergency of the given area, and also on the target groups to be prepared. The present study does not challenge discussing the preparation contents of every target group, therefore here I make a suggestion on the preparation of a broader range of population involved.

A *"broader range"* of population means citizens, who do not get involved in catastrophes through practising their vocation or fulfilling their duties, who are not members of civil defence organizations, but who are endangered by catastrophes. Obviously, the most of the population belongs here, that is why here I mean the concept "broad range". Naturally, the above group of citizens should be ranked according to their age, field of interest, state of health and, occasionally, occupation.

The *contents* of the preparations should be set to the *emergency specifications of the given settlement.* Their preparation serves the aim best in a *module scheme* as not everybody should be prepared to every task. Modules should carry, complex knowledge arranged centrally and deepened according to the local level of emergency. What *contents* would be probably needed by the population after an analysis of their emergency situation?

On the basis of catastrophe statistics and emergency managing practice, these are as follows:

- kinds of catastrophes, danger zones, behaviour rules to follow in emergency;
- alarming, scheme and methods of supplying information;
- physical and psychological effects of catastrophes;
- preparations for rescuing, rules and regulations of participating in a rescue action;
- Disaster Management and its collaborators;
- charge, discharge of civil defence;
- establishing civil defence organizations, rules of exertion;
- alarming the population, kinds of population defence and their roles;
- supporting bodies, organizations;
- fire-fighting, fire-prevention knowledge, first aid;
- opportunities of self-orientation, ways of asking for help, self-defence;
- localities, current issues, damage analysis, etc.

There are several ways to pass on this knowledge, and each of them needs special tools.[12] Tools and materials should always match contents.

Preparation periods

There is a professional debate on whether preparation is an activity of prevention. My point of view is that preparations have to be conveyed not only before catastrophes, but also during them, but in a special form, "embedded" in defence tasks. On the basis of this, I rank preparations according to periods:

Preparations in the preventive period

It means that the preparation activity is conveyed before an emergency, in a preventive period. Here the population is not only trained to obey the mechanisms of actions during an emergency. Beyond this, they should be given support in building up their skills in self-defence, as well as they should be made realize how to avoid causing emergencies themselves.

Preparations during emergency

It means that the preparation procedure is done in immediate danger or during an occuring emergency. If the preventive-period preparation scheme worked well, it is much easier to perform preparation during emergency. Most frequently it takes place in the form of information service. A unified information service guideline should be formed for various emergencies and catastrophes, which are actualized by Disaster Management specialists along with defence agencies in case of an occurring emergency, and information material and methods are worked out according to the specialities of the occurring emergency in order to inform and prepare the various target groups of the population effectively.

Preparations in the re-establishing period

It is conveyed after warding off a catastrophe or when the emergency is over. Besides the method of preparing the population for an existing or overhanging emergency, the preparation activity of the re-establishing period also has great importance. The population, whose lives are partly or completely deranged, are extremely defenceless. "Reorganizing" life requires fast

[12] Dr. Endre Sztanek, 2003.

and precise information flow, uniform administration, synchronized activities, and it also needs the population to be prepared for being aware of what to do for re-establishment and restoration to happen soon and with minor losses, they should know the losses and the extent of the reversibility or irreversibility of processes.

Methods of preparation

Selecting the appropriate preparation methodology is a crucial point, regarding the successfulness of the preparation. The population's preparation can be done through conveyance of knowledge, skills-developing or mixed-type drills or exercises.

- In *knowledge-conveying courses* "only" knowledge is passed on to the subjects of the preparations, which they accept either in an active or in a passive way.
- In *skills-developing courses sub-skills* are drilled which are needed for practicing the necessary rules of behaviour and activities followed or done in case a catastrophe bursts out. E.g. putting on a gas mask, drilling of crawling under smoke level, etc.
- In *mixed-type courses* both knowledge-conveying and skills-development are trained.
- In *exercises* complex practical tasks are solved in hold of the obtained knowledge.

In the following part I present a few population-preparation methods, out of which one can choose the most appropriate one for local conditions, target groups, own personality and financial resources. These are as follows (without aiming at completeness):

- giving lectures, persuasion;[13]
- presentation of Disaster Management equipment;
- organizing a visit to a fire-fighting barrack (introducing the methods of fire-prevention, fire-protection, fire-fighting);
- visiting of fire-fighter museums, and local civil-defence collections, giving lectures;
- preparing and publishing leaflets, educational issues;
- publishing educational material in written or electronic media;
- conducting adult or children competitions on defensive issues;
- organising exhibitions on the preparation of the population;
- participating in the programmes of other defence bodies and connecting their knowledge with catastrophe-related knowledge;
- preparing web-pages with the topic of the preparation of population;
- publishing study books or workbooks on emergency;
- holding lectures, special classes, drills in educational institutes;
- recruiting and preparing volunteering providers;
- founding and operating Security Information Centres (SIC), etc.

The above proposed knowledge can be broadened or narrowed according to the age and composition of the target group, but it is also important to work out appropriate practical tasks to each topic, which than could be practised by the participants.

SUMMARY

[13] Raymond Hull, 1997.

As a summary, regarding the *purpose of the preparation of the population*, it can be *claimed* that it is one of the most important issues of the Disaster Management activities, which nowadays falls on regular organizations, but well-prepared volunteering providers, mayor-supporters, civil organizations, feeling responsibility towards their community can also play an important role.

Tasks aiming at the protection of the population play a major role in the Disaster Management scheme. Among them the protection of the population is highly ranked during which the population is *prepared* for emergencies below and above a catastrophe threshold, skills are *trained* in them, with the help of which they can successfully rescue themselves or their mates, and their assets in these situations. *Furthermore*, defence knowledge and rescue abilities of the civilian population taking part in eliminating a catastrophe are *established*.

Its *most important purpose* is to *familiarize* the endangered citizens or those suffering from the harmful effects of a hazardous situation, and also the participants of the rescue operations with the emergency situations, the rules of behaviour and acting to follow, the methods of self-rescue and rescuing others and assets. It is clearly seen that it is a complex system of activities, which has various sub-systems. In a sub-system the providers, the subjects, the preparation material, the preparation periods, the preparation tasks and methods appear as further sub-systems. Their specifications are the basis for realising the preparation in a given area. The knowledge should be shaped according to the age range and composition of the target group and it should be conveyed in an appropriate way.

The task and responsibility is huge, only well-prepared specialists are able to cope effectively, who fulfil their duties professionally and with responsibility, and also conscientiously, and who approach the task from a systematic point of view.

"...each affair has its prospects: some, in order to tell them properly, should be seen closely, but others can only be told, if they are regarded from a distance."

Rochefoucauld

References

[1] Dr. Endre Sztanek: Handbook for Primary School Teachers Teaching Disaster Management and Civil Defence. Hungarian Civil Defence Alliance, Budapest, 2003., p. 56.

[2] Dr. Imre Varga: System of Actions on the Prevention and Protection against Serious Accidents due to Hazardous Materials. doctoral dissertation, p. 41., ZMNE, 2005.

[3] Gov. Decree 165/2003.(X.18.) About the Order of Informing the Population in Case of Nuclear or Radiological Emergency (Appendix 1. Point 1)

[4] Gov. Decree 2/2001(I. 17.) About Protection against Serious Accidents due to Hazardous Materials 16§ (2) and Modifications

[5] Júlia Hornyacsek-Viktória Veres: Theoretical and Practical Questions of Preparing the Population for Disaster Management, Vol. 1. ZMNE, Budapest, 2005. p. 3.

[6] Law 2011. CXXVIII. on Disaster Management and the Modification of Related Laws, Chapter IV., 30.§ (1)

[7] Raymond Hull: The Basics of Successful Public Speech, Budapest, Bagolyvar Publishing House, 1997. ISBN: 963-971-72-2

[8] Rezső Pellérdi: Challenge of our Era: the Nuclear Terrorism, Spring Wind Conference issue, Social Sciences. DOSZ, Budapest, 2007. p.469.

[9] Szilvia Csábi: Hungarian Concise Explanatory Dictionary, Akademiai Publishing House, Budapest, 2003. p.143.

[10] www.katasztrofavedelem.hu, (download: 03.10. 2011.)

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Kozma Zsolt - Huszár András
zsoltkozma67@gmail.com, andras.huszar@aok.pte.hu

A KATONAI BIOGENETIKA: A BIOTECHNOLÓGIA ÉS A MOLEKULÁRIS GENETIKA EREDMÉNYEINEK KATONAI ALKALMAZÁSAI

Absztrakt

A publikáció célja a biológiai és orvostudomány hadtudományhoz való interdiszciplináris kapcsolatát elemezve felvázolni olyan katonai alkalmazásokat, ahol a biotechnológia és a genetika (továbbiakban: biogenetika) eredményeit a hadiipar már használja, vagy ahol a belátható jövőben e tudás felhasználása bizonyosan bekövetkezik. Foglalkozunk a biogenetika prediktív szerepével a hadseregben, a genetikailag módosított anyagpusztító mikroorganizmusok lehetséges szerepével a katasztrófavédelemben, és a hadiipari elektronikai logisztika biogenetikai összefüggésével. Rámutatunk a kérdéskört szabályozó nemzetközi egyezmények kettős célú értelmezhetőségére, azaz vizsgáljuk, elfogadható-e jogilag a katonai biogenetika ún. (ön)védelmi célra történő alkalmazása. Nyomatékosítjuk, hogy a katonai biogenetikai tudás a jövő eredményes hadviselésének egyik fontos záloga lehet.

The aim of this publication is to analyse the interdisciplinarity of the biological and medical sciences to the military ones, and outline those military applications, where the results of the biotechnology and the molecular genetics (called: biogenetics) have already been used or certainly those will have been used by military forces in the reasonable future. We investigate the predictive role of biogenetics on the military field, and the role of genetically modified anti-material microorganisms in the catastrophe protection, followed by a short summary about biogenetical context of military industrial electronic-logistics. We signal it, that the human dedicated right of dispose of genetic personal information as owner, may get injured in the moment of entering into the military service. We stress, that the military biogenetical knowledge will be one of the most important pawns of warfare in nearly future.

***Kulcsszavak**: katonai biogenetika, prediktív genetikai szűrés ~ military biogenetics, predictive genetic screening*

A MOLEKULÁRIS GENETIKA KIALAKULÁSÁNAK ÉS FEJLŐDÉSÉNEK MÉRFÖLDKÖVEI

A címben jelzett témakör kifejtése nem nélkülözheti a humán genetikai felfedezések rövid áttekintését, tisztelegve sok XX. századi Nobel díjas tudós munkássága előtt.

„Az emberiség egy nagyszerű ajándékot kapott...Az emberi genomot, melyet az élet könyvének hívtak eddig, inkább kell az élet könyvtárának hívni, melyben kellő alázattal és kreativitással végzett felfedezésekkel találhatjuk meg azon könyveket, melyek segítenek bennünket Önnön magunk maghatározásában, és megtalálni pontos helyünket az Élet színes vásznán". Ezek a felvezető szerkesztői gondolatai a Science tudományos folyóirat azon számának [1], mely az emberiség eddigi talán legnagyobb vállalkozásának, a Human Genom Projectnek (Emberi Genom Terv, HGP) sikeres befejezését közölte. Az emberi örökítőanyag négy különböző, úgy nevezett nukleotid bázisból (adenin, guanin, citozin, timin) egymásután, általában szabálytalanul, egyes helyeken szabályosan váltakozva felépülő sorrendiségét, a genom szekvenciáját sikerült feltérképezni, több mint 3,5 milliárd bázispár meghatározásával. Milyen prerequizítumok kellettek a biológiai tudomány, és az emberiség története e csúcspontjának eléréséhez.

1859-ben Charles Darwin publikálta *A fajok eredete* [2], majd 1865-ben Gregor Mendel a *Növényhibridizációs kísérletek* című munkáját [3]. Mendel saját megfigyeléseinek fontosságát, melyek bizonyították: a jellegek öröklődéséért nem véletlenszerűen összeolvadó, hanem törvényszerűen viselkedő és diszkrét jellegű örökítő faktorok a felelősek, csak 1900-ban de Vries, H., Correns, C.E. és von Tschermak, E. fedezték ismét fel [4-6]. Sutton, W. S. a testisejtekben és az ivarsejtekben jelen levő többszörös kromoszómákként (a sejtmagok megfestésekor tapasztalt színes testecskékként) azonosította ezeket a részecskéket 1902-ben [7]. A genetika kifejezést egy brit biológus, Bateson, W. írta le először 1905-ben [8]. A genetika számítások alaptörvényt, a Hardy-Weinberg törvényt 1908-ban megalkotják [9,10]. 1910-ben a gének közvetlen kromoszómakötődését Morgan, T.H. igazolja [11]. 1913-ban Sturtevant, A. elkészíti az első kromoszómatérképet [12]. 1927-től H.J. Müller leírása után a génekben végbement fizikai változásokat mutációnak nevezzük [13]. 1928-ban Griffith F. felfedez egy molekulát, mely képes átjutni egyik baktériumból a másikba [14]. Tatum, E.L. és Beadle, G.W. kimutatják, hogy a gének fehérjéket kódolnak (ez válik 1941-ben a genetika centrális dogmájává) [15]. Avery, O.T., McLeod, C. és McCarty, M. a DNS-t, mint önálló genetikai entitást izolálják 1944-ben [16]. 1950-ben Chargaff, E. kimutatja, hogy a négy nukleotid nem állandó arányban található meg a nukleinsavakban, de az adenin mennyisége közel áll a timin mennyiségéhez [17]. Watson, J.D. és Crick, F. közlik a DNS dupla hélix szerkezetét [18]. Tjio, J.H. és Levan, A. igazolják 1956-ban, hogy a humán kromoszómaszám 46 [19]. 1961-ben bizonyítják be, hogy a genetikai kód tripletekbe rendeződik, és elkezdődik a génszótárazás [20]. 1970-ben a Haemophilius influenzae baktérium tanulmányozása közben felfedezik a restrikciós endonukleáz enzimeket, melyek segítségével lehetővé válik a DNS molekula mesterséges elvágása [21]. 1976-ban sikerült az első működő mesterséges gén előállítása [22]. 1977-ben Sanger, F., Gilbert, W. és Maxam, M. egymástól függetlenül DNS-t szekvenáltak [23,24]. 1983-ban Mullis, K. felfedezi a molekuláris biológia csodafegyverét, a polimeráz láncreakciót, mely lehetővé teszi egy kitüntetett DNS szakasz mesterséges megsokszorosítását [25]. 1986-ban Monaco A. és munkatársai azonosítják a Duchenne izomdisztrófia gén szerkezetét a X. kromoszómában [26], 1989-ben Kerem és munkatársai a cisztikus fibrózis betegség génjét azonosítják a VII. kromoszómán [27]. 1995-ben a Haemophilus influenzae baktérium az első élőlény, melynek bázissorendjét rögzítik [28]. 2001-ben a humán genom sorrendiség első eredményét párhuzamosan készíti el a HGP és a Celera Genomics [29,30], majd 2003. április 14-én a HGP sikeresen befejeződött.

A genomok „annotálása” zajlik jelenleg, vagyis funkciójukat megismerve egy adott emberi kromoszóma adott helyéhez kell rendelni azokat. E korszak három legfontosabb kutatási iránya: a „proteomika”; mely lehetővé teszi több ezer emberi fehérje genetikai sajátosságainak megismerését, a „funkcionális genomika”; mely bioinformációs eszközökkel (nevük microarrays, DNS chipek) a poligénes öröklődésű kórképek és többszörös mutációk elemzését végzi; és a „farmakogenetika”; a genetikai hibák felismerése után új genetikai alapú gyógyászati módszerek kidolgozása [31].

A biotechnológiai kutatásoknak a molekuláris genetikához hasonló, igen gyors fejlődése, egy új tudományág, a biogenetika alapjait teremtette meg a XXI. századra.

A BIOGENETIKA KATONAI ALKALMAZÁSA

A biogenetikai technológiák rendelkezésre állnak a XXI. században ahhoz, hogy katonai alkalmazások céljára kinyerjünk információt a feltérképezett humán emberi, állati vagy növényi genomból, vagy vizsgálhassuk, különböző vegyi, környezeti ártalmaknak a genom integritására gyakorolt hatását, vagy éppen arra, hogy a genom előnyös vagy ártó jellegű mesterséges megváltoztatásával, egy mindenkori aktuális szándék mentén legyünk képesek mérnöki módon manipulálni a 2003-ban megtalált „életkönyvtárat”. A katonai alkalmazásoknak, ma már, szinte csak a képzelet szabhat elméleti, és a nemzetközi egyezmények jogi határt.

A biogenetika katonai alkalmazásainak csoportosítása

- Hadászati célú alkalmazások (1. táblázat):
  - Az alkalmazott haditechnika fejlesztése:
    - a védelmi képesség fokozása
    - a támadó képesség fokozása
- Személyazonosítás:
  - Katonai tömegsírok feltárása
  - Háborús áldozatok egyedi személyazonosítása, holttest vagy testrészek alapján
  - Katonai tömegkatasztrófák (pl.: repülőgép-szerencsétlenség) áldozatainak azonosítása
  - Harc a terrorizmus ellen (egyedi személyazonosítás, főbb használt módszerek: 1./ Genotipizálás: STR (short tandem repeat) vagy SNP (single nucleotid polimorfizmus) alkalmazása, 2./ Mitochondriális DNS alkalmazása sérült, vagy bomlott kis kópiaszámú biológiai minták esetén, 3./ DNS fenotipizálás: emberi tulajdonságok, hajlamok genetikai megközelítése, emberi külső jegyek genetikai elemzése)
- Katonai logisztika:
  - hamisítások elleni védelem
- Katasztrófavédelem:
  - A kármentesítés (bioremediáció) új dimenziói
- Prediktív katonai alkalmazások:
  - A katonák egyéni képességének legmagasabb szintű biztosítása:
    - biogenetikai szűrővizsgálatok
  - az alkalmazni kívánt vegyi anyagok vizsgálati lehetőségei a carcinogenezis, a mutagenezis és teratogenezis szempontjából

Az alkalmazás	Jellemzés
Elrejtőzés, álcázás	"lopakodó" képességgel bíró biológiai anyagok, festékek, egyéb fedőanyagok alkalmazása
Harcközbeni azonosítás	biológiai jelzők, melyek segítenek az ellenséges szándékú katonák kiszűrésében
Számítástechnika	DNS alapú számítógépek speciális igények megoldására
Adategyesítés	kiegészítő biomolekuláris memóriák kialakítása, mesterséges intelligencia
Funkcióval bíró ételek	táplálkozás-kiegészítők, emésztés fokozók, energiaraktározást növelők, harctéri azonosítás képessége, felismerhetőség csökkentők, ehető oltóanyagok, gyorsan növekedő növények
Egészség monitorizálás	egészségi állapotjelző eszközök, gyógyítási rangsor felállításának képessége, külső érzékelőkkel való állandó kapcsolat a környezet biológiai vegyi és egyéb ártalmainak felismerésére
Nagy kapacitású adattárolás	robosztus számítógép memóriák minden egyes katonának
Nagy felbontású képalkotás	alternatív biotechnológiai utak a félvezetőkön alapuló képalkotással szemben
Kissúlyú fegyverzet	a katonák és a fegyverzet védelmében öngyógyító biológiai rendszerek fejlesztése
Új anyagok	biológiailag hasznosítható fogyóeszközök, genetikailag módosított fehérjék, megújuló anyagok
Teljesítményfokozás	agyi implantátumok, számítógép beviteli és kijelző modulok alkalmazása, egyéni érzékelés növelése, ellenanyagok beépítése, génműködés ellenőrzése,
Sugárzásbiztos elektronika	fehérje alapú komponensek alkalmazása, biomolekuláris vegyes rendszerek alkalmazása, biomolekuláris diódák, biológiai FET-ek alkalmazása (FET: field effect transistors) teljesítménynövelő gyógyszerek
Miniatürizálás	sejtszintű folyamatok, molekuláris elektronika, biochipek, nanotechnológia
Harctéri környezet letapogatása	biochip laboratóriumok: harctéri kémiai-, biológiai és egyéb környezeti ártalmak azonnali, molekuláris szintű érzékelése és azonosítása
Oltóanyag-fejlesztés	Nem szokványos helyen történő hadviselés esetén, nem ismert kórokozók elleni oltóanyag gyors kifejlesztésének és gyártásának képessége,
Sebgyógyulás	Mesterséges bőr, és szervek előállítása, sebkezelésben a vérzéselállítás és a sebgyógyulás folyamatának gyorsítása

Az alkalmazás	Jellemzés
Érzékelők hálózata	harci eszközök és katonák által szállított távirányítható érzékelők harctéri alkalmazása
Katonai gyógyszerek	shock elleni szerek, genetikai alapú gyógykezelési módok, oltóanyagok hatékonyságának optimalizálása
Hordozható erőforrások	biológiai alapú "fényelőállítás", sejtalapú energiaforrások
Célfelismerés képessége	Fehérje alapú mintafelismerő eszközök, mesterséges intelligencia

1. táblázat. A biogenetikai eredmények lehetséges katonai alkalmazási területei az USA hadseregében 2001-2026

Forrás: Opportunities in biotechnology for future army application
ISBN-10: 0-309-08678-7, 74. oldalon található 8-1 sz. táblázat alapján

Jelen publikációnkban a katonai elektronikai logisztika-, a bioremediáció biogenetikai aspektusait, és a prediktív katonai genetikai alkalmazások közül a lehetséges biogenetikai szűrővizsgálatok elemzésére vállalkozunk.

A KATONAI ELEKTRONIKAI LOGISZTIKA BIOGENETIKAI DIMENZIÓI

A katonai hadászati technológiák nem nélkülözhetik bonyolult informatikai infrastruktúrák mindennapi alkalmazását. Különösen fontos hogy az ezekben elhelyezett elektronikai alkatrészek, áramkörök, félvezetők, chipek a gyártók specifikációinak megfelelő, és a felhasználók által elvárt, megbízható módon működjenek. Ez ellen hathat a termékek illegális másolása, majd kereskedelme. Ma már bizonyos, hogy egy új elektronikai termék megjelenésével szinte egyidőben jelennek meg a hamisítványok, sok esetben nagyobb hasznot hozva a „kalóz" gyártóknak, mint a termék jogtulajdonosának. A Nemzetközi Kereskedelmi Kamara (International Chamber of Commerce) 2011. februári jelentése arra figyelmeztet, hogy a hamisítás mértéke a világkereskedelem 5-7 %-ra is rúghat és 4 éven belül elérheti az 1,7 trillió dollárt, évente 2,500.000 legális munkahelyet veszélyeztetve a világon [32].

Az USA Tengerészeti Minisztériuma az USA Kereskedelmi Minisztériumával együtt – a világon eddig elvégzett legnagyobb volumenű ellenőrzés keretében, 2007-2010 között, megvizsgálta az USA védelmi minisztériumának elektronikai jellegű beszerzéseire és a termékek felhasználásra vonatkozó logisztikai útjait a hamisított elektronikai termékek használatának jellegére, mértékére vonatkozóan. A 2010. januári összefoglaló jelentés három legfőbb megállapítása volt [33]:

- Az USA hadseregének összes katonai logisztikai útja, mely elektronikai termékek beszerzésével és telepítésével, felhasználásával foglalkozik kivétel nélkül és közvetlenül érintett hamisított termékekkel.
- Az eddigieknél szorosabb ellenőrzési utak és belső protokollok kialakítása indokolt ezek megszüntetésére.
- A termékek eredetiségjelölésére minden eddigi törekvésnél biztonságosabb megoldásokat kell keresni a gyártók, közvetítők, és eladók bevonása mellett.

Az egyedi termékjelöléseknek hosszú ideig, megbízható módon kell lehetővé tenni a termékek egyedi ujjlenyomathoz hasonlítható, hamisíthatatlan jelöléseit, mindezt úgy, hogy saját kémiai összetételük semmilyen hatással se lehessen a jelölni kívánt elektronikai alkatrész specifikus jellemzőire. Az egyediséget tovább erősítheti, hogy a termék bármely részösszetevője – függetlenül annak anyagától, szerkezetétől – jelölhető legyen, és a jelölés a kereskedelmi, logisztikai útvonal esetleges szélsőséges környezeti hatásaival szemben is

ellenálló legyen (pl.: szállítás közben előforduló jelentős hőmérséklet-, légnyomáskülönbségek, repülőtéri átvilágító szerkezetek röntgensugár-hatásai, tengerek sós párás környezeti hatásai, többszöri átrakodás mechanikai traumái).

Az eddig alkalmazott holografikus eredetjelölők, vagy egyéb, a külső csomagoláson alkalmazott jelölések önmagukban is könnyen hamisíthatók, a belső jelölések közül pedig az ásványi anyag molekulákkal történő jelölések, vagy a nanotechnológiában kifejlesztett ferrit ionos jelölések [34] felhasználása – a fenti elvárások figyelembevételével - limitált.

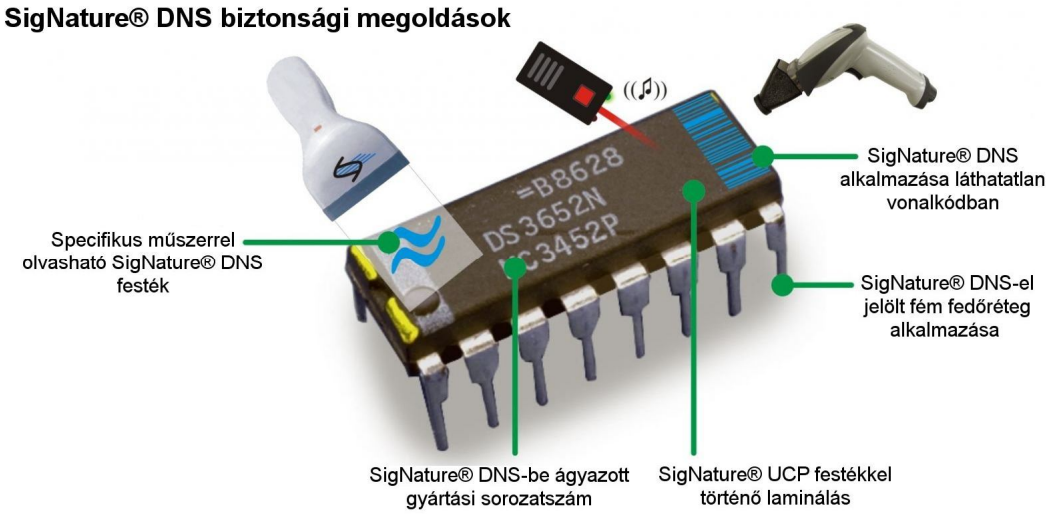
Ma már köztudomású is, és a joghatóságok által az egész világon elfogadott tézis, hogy a DNS alapú ujjlenyomat-technika egyedi személyazonosítást tesz lehetővé. A mai standardizált laboratóriumi technikákkal minden olyan biológiai anyag, melyben az egyén sejtmagja megtalálható (nyál, haj, vér, izzadság, vizelet, szövetdarab) alkalmas ezen egyedi információ kinyerésére (a fals pozitív eredmény esélye 1:3 trillióhoz). Sejtmaggal azonban a növényvilág egyedei is rendelkeznek. Az ezekből nyert DNS szakaszok tekintettel a növényi egyedek sokszínűségére ugyancsak alkalmasak az egyedi jelölésekre, és megfelelő technológiákkal stabilitásuk extrém körülmények között is megteremthető.

Az Applied DNA Sciences (Stony Brook, N.Y., USA: hivatalos rövidítése: APDN) cég 2009-2010 között fejlesztette ki növényi DNS eredetű jelölő technológiáját, mely minden eddigi, az elektronikai alkatrészek eredetiségjelölésével kapcsolatban felállított, megkövetelt feltételnek megfelel [35] (2. táblázat).

Teszt	**A kísérlet jellemzői**	**Eredmények**
UV behatás	Denver várost 350 év alatt érő UV hatással azonos erősség	Stabil
Röntgen besugárzás	repülőterek röntgen szkennerjeihez mért 4 x-es sugárerősség	Stabil
γ-sugárzás	30 kGy (kilo-gray) erősségű behatás sterilizáló készülékkel	Stabil
pH hatás	1 napos behatás különböző pH erősségű oldattal (pH 1- pH 14)	Stabil
Hőhatás	250 Celsius fokos maximum hatásig vizsgálták	Stabil

2. táblázat. Az APDN által alkalmazott növényi DNS alapú jelölők stabilitásvizsgálata (Applied DNA Sciences, Inc.)
Forrás:
http://www.adnas.com/sites/default/files/files/DNA%20to%20Safeguard%20Electronics%20Against%20Counterfeiting%20June%2020%202011%281%29.pdf, (letöltve: 2011.06.28.)

Az elhelyezett azonosító nem másolható, és biogenetikai manipulációkkal (pl.: complementer DNS szál felépítése) sem reprodukálható. A gyár legújabb szabadalma lehetővé teszi az ipari technikában mindenütt alkalmazott cián-akrilát tartalmú ragasztókba való beágyazását e növényi DNS jelölőknek, és a ragasztóból való visszanyerést is [36]. E növényi eredetű egyedi DNS szakaszok nem igénylik a gyártási folyamatok megváltoztatását, szinte bármely hordozó felületre felvihetők, és jelenlétük egyszerű módon – kézi ultraibolya-sugárzást kibocsátó készülékkel – feltárható (1. ábra).



1. ábra. DNS alapú jelölések lehetőségei mikrochipeken.
Forrás: http://www.adnas.com/Blog/electronic-and-electrical-components, (letöltve: 2011.06.28)

Az ily módon azonosított eszközök, alkatrészek egyedi vizsgálata a fejlesztő cég laboratóriumában lehetséges, mivel a detektálási technológiai folyamat is szabadalmi oltalom alatt áll.

Az USA Védelmi Minisztériuma javaslatára, kétéves teljeskörű megfelelőségi vizsgálatot követően a Védelmi Logisztikai Hivatal, 2011-től, 1 millió dolláros keretet nyitott meg a cég számára, melyet az USA minden kormányzati szerve elektronikai logisztikai beszerzési láncában a növényi eredetű DNS alapú (SigNature®: Applied DNA Sciences védjegye) eredetjelölés megvalósítására kell fordítani [37].

A BIOLÓGIAI LEBONTÁS ÉS KÁRMENTESÍTÉS BIOGENETIKAI DIMENZIÓI

A hatályos nemzetközi egyezmények – különösen a Biológiai és Toxin Fegyverek Konvenciója (BTFK) [38] és a Cartagena Biobiztonsági Protokol (CBP) [39] – egyértelműen tiltják emberek, állatok vagy növények elpusztítására alkalmas anyagok, molekulák, élőlények támadó céllal történő előállítását, tartását, kereskedését vagy ilyen célból a természetben élő biológiai élőlények módosítását. A nemzetközi egyezmények szövegének napjainkban felbukkanó szabadabb, vagy egyoldalúbb értelmezései (kettős mérce=dual purposes), azonban a XX-XXI. század egyik jelentős tudományos területévé tette a környezetünk anyagai ellen felhasználható genetikailag módosított-, vagy előállított mikroorganizmusok (baktériumok, gombák: továbbiakban mikrobák) kutatását, biogenetikai módosítását, és a hatékonynak bizonyulók gyakorlati alkalmazását.

Miben áll a dual purposes jelenség. A direkt tiltás alapján tehát nem lehetne ilyen kutatásokat végezni egyáltalán, hisz a támadó célra alkalmazhatóság elvi lehetősége igen nehezen zárható ki abból a folyamatból – különösen a teljesen befejezett tudományos projectek esetén –, amely ilyen technológiák kifejlesztésével előáll. Szólnak meggyőző érvek amellett azonban, hogy megfelelő biztonsági szintek felállítása esetén elérhető, hogy az anyagpusztító technológiákra vonatkozó, katonai célú kutatások és alkalmazások kizárólag védelmi célokat szolgáljanak, azaz felkészülést olyan esetleges támadásokra, amely ilyen támadó eszközökkel történhet olyan fél (országok, csoportok) által, ahol ezen anyagok,

támadó katonai célú fejlesztését jogszabály nem tiltja, vagy olyan országok részéről, amelyek nem aláírói a nemzetközi tiltó egyezményeknek.

A jogi szabályozás egyedi, felpuhított értelmezései azonban oda is vezethetnek, hogy ezek a folyamatok kicsúszhatnak a tudomány és a békés katonai alkalmazás berkeiből és végeredményben ezen anyagok ún. biológiai anyagpusztító fegyverek kifejlesztését szolgálhatják. Látni kell, hogy ugyanazok az új genetikai jellemzők, amelyek alkalmassá, és hatékonnyá teszik a génmódosított mikroorganizmusokat a békés célú, biológiai tisztító, újrahasznosító folyamatokban való alkalmazásra, akár a katonai katasztrófavédelemi kármentesítésben, ugyanezen jellemzőik alapján válhatnak alkalmassá biológiai – közvetlenül nem halálos – fegyverként való alkalmazásra is.

Különleges katasztrófavédelmi feladat, továbbá az ezeket a genetikailag módosított élőlényeket előállító laboratóriumok, gyárak védelmi rendszerének tervezése, a biztosítás megszervezése, vagy egy katasztrófa esetén e speciális fertőzöttség felszámolásának biztosítása.

A világ szinte minden anyaga lebontható biológiai alapú folyamattal. Az épített infrastruktúra ellen ható aktív mikrobák is ismertek, erre példa a szénhidrogéneket kedvelő baktérium, amely óriási lyukakat képes emészteni az aszfaltban, hozzájárulva az útfelszínek lebontásához [40]. Egyes mikrobák képesek elindítani a haditechnikai, vagy katasztrófavédelmi üzemanyag-ellátó rendszerek lebontását, vagy katonai repülőgépekben alkalmazott kompozit, lopakodó technológiák károsítását mediálni [41,42]. A beton szintén egy olyan anyag, amelynek károsítása, lebontása hatalmas katasztrófavédelmi problémát is jelenthet [43]. A Thyobacillus ferrooxidans és más mikrobák vas-réz-és cink fémionokat halmoznak fel élettani folyamataik során [44], melyek a katonai haditechnikában az elektronikai berendezések, chipek beláthatatlan következményekkel járó pusztításait eredményezhetik. Az ismert mikrobák közül számos képes viszonylag gyors és hatékony lebontásra, pl. szénhidrogének, műanyagok, néhány esetben fémek egy-két hét, vagy egy-két hónap alatti lebontására.

A lebontó mikroorganizmusokat hasznos célra is alkalmazhatja az emberiség, és a katonaság pl. szennyező anyagok lebontására, átalakítására, azaz a kármentesítésre [45]. Ezt a szakirodalom bioremediációnak (biológiai kármentesítésnek) hívja, mely folyamaton azt kell érteni, hogy bizonyos mikrobák képesek egy adott szennyező anyagot – egy összetett közegben - célzottan lebontani, olyanokat is, amelyeket más módon szinte lehetetlen.

Természetes valójukban az e célra használható mikrobák is igen lassú folyamatok során hatnak, de a biotechnológia képes olyan genetikai módosításokat létrehozni, hogy ez a funkciójuk felgyorsuljon. És itt már kézzel foghatóvá válik a „kettős mérce” veszélye. A tisztítókapacitás vagy potenciál felerősítése miatt a békés célú alkalmazások mellett megjelenik egy virtuális, eltérő alkalmazhatóság lehetősége, ezen módosított mikrobák fegyverként való alkalmazása hadászati céllal a szembenálló fél által épített vagy elfoglalt műtárgyak-, vagy egy elfoglalni kívánt terület anyagainak lebontása céljából.

A világ országainak egyező az álláspontja, hogy erősen szennyezett környezetet eredményező katasztrófahelyzetben – anyagpusztító természetű mikrobák használatával – a katonai szerepvállalásnak, akár ipari méretű folyamatok alkalmazásának is helye lehet a kellő hatékonyságú védelmi, elhárítási feladatok biztosításában. Ilyen megjelölt környezeti problémák, beleértve a sugárfertőzöttséget, szénhidrogénekkel vagy egyéb kémiai anyagokkal történő kontamináció elhárítását, lehetőséget adtak a múltban is és jelenleg is olyan kutatások végzésére, amelyek az előzőekben említett mikroorganizmusoknak a szennyezés elpusztítására való hatását, hatékonyságát vizsgálták, vagy ilyen irányú fejlesztéseket lehetővé tettek. Ilyen példaként hozható a TNT (2,4,6-trinitro-toluol) által okozott szennyezés megszüntetése fertőzött környezetben. Ilyen eset békeidőben katonai lőszergyárakat, vagy

lőszerraktárakat ért katasztrófahelyzetekben, vagy katonai gyakorlóterületeken, vagy katonai háborús helyzetben hadászati cselekményeket követően állhat elő. Ilyen TNT bekebelező mikrobák közül a tudomány már számosat izolált [46], és közülük több annyira hatékony, hogy hét nap alatt az eredeti TNT hatáserősségét 50%-kal képes csökkenteni. Ez a fokú hatékonyság még a kivételek közé tartozik.

Tudományosan inkább az állítható, hogy természetben előforduló, ilyen képességekkel rendelkező mikrobák alapvetően ineffektívek biológiai kármentesítésre, azaz csak rendkívül lassan, előre nem szabályozható sebességgel és ideális környezeti körülmények esetén képesek kifejteni ilyen területen hatásukat. A biogenetika lehetősége (egyben veszélye) abban rejlik, hogy megtalálják azokat a genetikai kódokat, géneket, amelyek egy adott mikroba hatékony célmolekuláját, vagy a funkciógyorsaságát kódolják, és ezek megváltoztatásával az előbb említett célokra hatékony törzseket állítsanak elő.

Az élő organizmusok szabadalmi oltalommal való védhetőségében az Amerikai Egyesült Államok mérföldkőnek számító alapesete egy olajbontó - genetikailag módosított - baktériumra beadott szabadalom volt (US Patent 4259444, 31.03.1980) [47]. Később a kutatások a természetben előforduló baktériumok szelekcióját, illetve a megfelelőnek talált törzsek szaporítását, nagy tömegben történő gazdaságos előállítását célozták. A legtöbb ilyen kutatás középpontjába a radioaktívan szennyezett területek megtisztításának problémája került. 1998-ban közölték a radioaktív környezetnek ellenálló baktérium, a Deinococcus radiodurans genomjának szerkezetét [48]. Más tudósok szén-tetraklorid és nehézfém mérgezések esetén ezen anyagok lebontásában szerepet játszó mikroorganizmusokat tenyésztettek, mások genetikailag módosított mikrobákat alkalmaztak PCB-k (poliklórozott bifenil molekulák) lebontására [49]. További kutatások pedig olyan mikroorganizmusokat is találtak, amelyek ún. inklúziós testecskéket, só, fém vagy műanyag tartalmú granulumokat képesek előállítani élettani folyamataik során, amelyek az alkalmazott hadászati technika alapköveinél, az integrált áramköröknél, processzoroknál fejtik ki hatásukat, ezzel okozva közvetlen, vagy közvetett környezeti katasztrófát [50].

Az anyagpusztító természetű genetikailag módosított molekulákban rejlő gazdasági és katonai potenciál szinte beláthatatlan. Kifejleszthetők a mai technológiai színvonalon olyan mikrobák amelyek minden korábbinál hatékonyabban válnak alkalmassá szénhidrogének, műanyagok, természetes vagy szintetikus gumi, a fémek és kompozit anyagok lebontására, vagy képesek lerombolni hidakat, autópályákat – legyen az betonból vagy aszfaltból – fém alkatrészeket, fedőanyagokat, gumit vagy fegyverek más alkotóelemeit, közlekedési eszközöket – beleértve repülőgépeket – és az ezeket kiszolgáló felszereléseket. Képesek tönkretenni az üzemanyag utánpótlást, magát az üzemanyagot vagy az ezt helyettesítő energiaforrásokat, vagy dugulást előidézve szűrőberendezéseket, filtereket. Mesterségesen előállított, összetett ötvözeteket, festékeket, védőrétegeket vagy akár modern műanyag alkotórészeket pusztíthatnak csendben észrevétlenül. Mindezek a kutatások elérhető közelségbe hozták nem csak a hatékony civil alkalmazásokat, hanem a kifejezett katonai alkalmazási lehetőségeket is. A katonai célú alkalmazások esetén azonban hangsúlyt kell helyezni arra, hogy ezek a kutatások védelmi célt szolgál(ja)nak és ennek minden jogi biztosítékát meg kell teremteni tekintettel arra, hogy a hatályos nemzetközi egyezmények bármilyen támadó célú alkalmazását ilyen mikroorganizmusoknak tiltják.

A kutatások még két fontos irányba mozdultak el. Az egyik a hatékony, genetikailag módosított, anyagpusztító technológiák adott alkalmazási területen történő, minél hatékonyabb szétszórását, azaz a konkrét alkalmazás megkönnyítését segítik (mikrokapszula, nanotechnika), valamint a módosított baktériumok és gombák életfunkciói megszűnésének tervezhetősége irányába. Ez utóbbi területen az áttörést a Streptomyces avidinii streptavidin génjének beültethetősége jelenti az élő organizmusok genomjába, mellyel az adott élőlények

gyors programozott halálát lehet előidézni, bármely olyan esetben ahol az adott mikroba nem talál saját környezetében az alapfunkciójának ellátásához szükséges molekulákat. A technológia – egy furcsa történelmi véletlen(!?) – épp azon a napon kapott szabadalmi védelmet az USA-ban, amikor az meghirdette a terrorizmus elleni harcának kezdetét, 2001. szeptember 11-én (US Patent 6287844) [51,52].

A KATONAI PREDIKTÍV BIOGENETIKA

A „tökéletes katona mítosza" foglalkoztatja a katonai tudományos életet [53]. A biogenetikai eredmények közvetlen felhasználása a katonai szűrővizsgálatokban kézzelfogható közelségbe hozta, hogy a fantáziából valóság lehessen. Azokban az országokban azonban, ahol nem különül el az állampolgárok genetikai információival kapcsolatos önálló rendelkezési joga attól függően, hogy civil vagy katonai jellegű alkalmazásról van szó, a mítosz még sokáig mítosz marad.

Az USA 2008-ban elfogadott genetikai információs törvénye (Genetic Information Nondiscrimination Act, GINA) [54] azonban a genetikai információk korlátlan, illetve a személy beleegyezése nélküli felhasználásának tilalmát a katonai alkalmazásokra közvetlenül nem terjesztette ki. Mindez lehetővé teheti annak a múltbéli gyakorlatnak a formalizálását, hogy a katonai szolgálat létesítésének pillanatában a katonák által az USA-ban kötelező jelleggel adandó DNS minták, ne csak a mindenki számára 1991 óta ismert célból (katonai áldozatok genetikai alapú személyazonosíthatóságának megteremtése az USA Katonai DNS Adatbázisa alapján) vagy a Nemzetvédelmi Törvény 2003-as kibővítése utáni célból (bírósági jogi eljárásban, megalapozott gyanú esetén, ha más biológiai bizonyíték alapján nem lehet egy ügyet befejezni felhasználható egy személy USA katonai DNS adatbázisában raktározott mintája az adott jogi eljárásban) [55]), hanem prediktív genetikai szűrésre is felhasználhatók legyenek.

A genetikai előrejelzésnek hadászati jelentősége van, mely az alábbiakban foglalható össze:

- Minden katonai operációban a lehető legalkalmasabb (genetikai és testi értelemben a lehető legegészségesebb) katona kerüljön bevetésre.
- Egyébként kiváló katonákat ne alkalmazzunk olyan speciális környezetben, amely a meglévő genetikai adottsága alapján egy kórkép, betegség kifejlődésének nagyfokú valószínűségét rejti magában.
- Ne alkalmazzunk katonai szolgálatra egyáltalán olyan személyt, akinek genetikai adottságai alapján a szolgálat (annak alaptermészetéből adódóan) igen nagy valószínűséggel okoz maradandó egészségkárosodást.

A prediktív genetika másoldalról segítséget jelenthet a katonai szolgálat alatt kialakult betegségek utáni, polgárjogi kártérítési igények pontosabb elemzéséhez, és egyes országokban az ilyen típusú pénzbeni kifizetések (járadékok, nem vagyoni kárigények) mértékének mérsékléséhez.

Az elérhető –elsősorban az amerikai hadsereg gyakorlatára – vonatkozó források alapján három csoportba sorolhatók a katonai alkalmazások:

- Az alábbi kórképekre genetikai szűrés történik [56a]:
  - Glükóz-6 foszfát dehidrogenáz enzimhiány és
  - Sarlósejtes vérszegénység
- Az alábbi kórképek katonai biogenetikai értékelése megtörtént adott jogesetek kapcsán, de rutinszerű előszűrések alkalmazására nincs egyértelmű adat [57a]:
  - Von Hippel-Lindau szindróma

- Gyűjtőér-rögösödés, és tüdőembólia bekövetkeztének esélyét emelő genetikai mutációk:
    - aktivált protein C (APC) rezisztenciát okozó Faktor V R506Q (FV Leiden) mutáció
    - prothrombin gén G20210A mutációja
    - a metilén-tetrahidrofolát-reduktáz (MTHFR) enzim génjének pontmutációja (C677T)
    - a cisztationin-béta-szintáz (CBS) gén mutációja

- 3. Az alábbi multigénes öröklődésű kórképek részletes vizsgálata, a genetikai és környezeti hatások arányának meghatározása céljából folyamatban van. Világszerte ezen kórképek esetén a legmagasabb a leszerelés után megítélt és fizetett járadék-, és kártérítési összeg:
    - Poszttraumás stressz betegség [58,59]
    - Csukló alagút szindróma (az alkari középideg motoros és/vagy érző funkciójának tartós károsodása) [60]

AZ 1. ÉS 2. CSOPORTBA SOROLT KÓRKÉPEK KATONAI BIOGENETIKAI JELENTŐSÉGÉRŐL

Glükóz-6 foszfát dehidrogenáz (G6PD) enzimhiány:

Az X kromoszómához kötötten (a gén a hosszú kar Xq28 pozíciójában található), recesszíven öröklődő betegség, mely a világon kb.400 millió embert érint. A hibás allélek előfordulási gyakorisága, melyeket intronmutációk okoznak, szoros kapcsolatot mutat a világ maláriafertőzött területeinek határával. A betegekben az oxigénszállító vörösvértestek széteséséhez társuló haemolitikus krízis következik be, sokszor halálos veseelégtelenséggel szövődve, melyhez egy sokáig tünetmentes egyénnél számos stresszorhatás vezet. Akár maláriaellenes szerek (primaquine, pamaquine, chloroquine), vagy szulfonamidok (szulfanilamid, sulfamethoxazole, mafenide), tiazo-szulfonátok, metilénkék, naftalin, számos fájdalomcsillapító (aszpirin, phenazopyridin, acetanilid), de a hennafestés alkalmazása, vagy bizonyos ételek fogyasztása (mediterrán régiókban a fava bab) is előidézheti a betegség tüneteit.

Ismert katonai biogenetikai gyakorlat: Az USA hadseregébe belépő személyek mindegyikét kötelezően vizsgálják G6PD hiányra. A pozitív (hibás gént hordozó) esetekben ennek tényét a katonák orvosi dokumentumában és „dog tag”-jén is rögzítik. Ilyen előzmények esetén a katonát nem küldik bevetésre malária fertőzött területekre, ahol primaquine, pamaquine, chloroquine szer adására van esély, esetleges gyógykezelésüknél az oxidatív stresszor gyógyszerek adását kerülik [56b]

Sarlósejtes (sickle cell) vérszegénység:

Autoszómális recesszív módon öröklődő pontmutáció okozza a hemoglobin béta génben, a 11. kromoszóma 11p15.5 pozíciójában, mely a hemoglobin S (HbS) termelődéséhez vezet. A hemoglobin a vörösvértestek (VVT) belsejében található vastartalmú fehérje. Oxigént szállít a tüdőktől a test minden részébe, és leadja azt a szervezet szövetei és sejtjei számára. A hemoglobin gén mutációja a VVT belsejében található folyadékban kevésbé oldódó hemoglobin képződését eredményezi, amely az oxigénszállítás normális szakaszai során polimerizálódhat. A polimerek kialakulásuk után nem képesek visszaalakulni, és az oldhatatlan HbS miatt az oxigénszállítás megszűnik. A gyakori szövődmények egyike az úgynevezett „sarlósejtes krízis”, amely elsősorban a hosszú csövescsontok fájdalmával jár. Leggyakrabban a következő okok válthatják ki: az oxigén kínálat csökkenése, fertőzés,

kiszáradás, (földrajzi) magassági változás, és hőmérsékleti szélsőségek. A sarlósejtes vérszegénységben a három szövődmény, amelytől leginkább tartani kell: a stroke, a heveny mellkasi szindróma, és a fertőzések.

Ismert katonai biogenetikai gyakorlat: Az USA hadseregébe belépő személyek mindegyikének genomját kötelező jelleggel vizsgálják sarlósejtes vérszegénység irányába. A pozitív (hibás gént hordozó) esetekben ennek tényét a katonák orvosi dokumentumában és „dog tag"-jén is rögzítik. Ilyen előzmények esetén a katonát, az adott haderőnem követelményeire figyelemmel, vagy fel sem veszik a szolgálatba, vagy szolgálatát felfüggesztik, vagy kiképzéskor a stresszor tényezőket kiiktatják, pl.: magaslati táborokba nem küldik őket, külön figyelnek a fizikális tréningek során fellépő tüneteikre (egyes kiképzőhelyeken piros karszalagot viselhetnek, mellyel jelzik kiképzőtisztjüknek genetikai érzékenységüket stresszor hatásokra) [56c].

von Hippel-Lindau szindróma(VHL):

Autoszóm domináns öröklődésű kórkép mely a 3. kromoszóma 3p26-p25 pozíciójában egy hírvivő RNS-t kódol, mely a sejt citoplazmájában egy fehérje meghatározásában vesz részt. Hibás allélek esetén, a normál sejtműködés több pontján, okoz e fehérjehiány zavart, de nem ez, hanem rosszindulatú daganatok kialakulásban betöltött szerepe teszi igazán veszélyessé a betegséget. Az érintett személyek 75 %-ában vesekarcinóma, 70 %-ában központi idegrendszeri éreredetű daganat (haemangioblasztóma), kisebb részükben szem ideghártya vagy középfül eredetű haemangioblasztóma alakul ki.

Ismert katonai biogenetikai eset: A prediktív katonai genetika alapesetének számít a Jay Platt versus United States Marine Corps eset. A tengerészeti kiképzőtisztnél 15 év szolgálat után 32 évesen diagnosztizálták, 1998-ban, a VHL-t, és az akkor érvényben volt belső szabályozás szerint (US Department of Defense Instruction 1332.38/1996/E.3.P.4.5.2.2./) semmilyen további egészségügyi ellátást nem fizettek részére, szolgálatát anyagi kompenzáció nélkül megszüntették – fizikai alkalmatlanságra hivatkozva – az alapján, hogy esetében a daganatos betegség előfeltételei már 17 éves korára bizonyosan kialakultak. Platt, többszöri agy és veseműtét után, fél szemére megvakulva magaslati hegyi túrarekordokat állított fel, karját és lábát átkötve harmadikként a világon átúszta a San-Franciscói Alcatraz öbölt, de nem tudott újra szolgálatba lépni. A későbbi jogi eljárásnak két döntő következménye lett a későbbi általános gyakorlatra: 1./ Az USA Haditengerészete elfogadta azokat a tudományos érveket, hogy esetében a genetikai adottság manifesztálódásához a 15 év szolgálat alatt, a kiküldetésekhez társult többszörös vakcináció, valamint a fegyverek tisztításához használt anyagok toxikus hatása is hozzájárulhatott. 2./ 2005-ben az USA hadügyminisztériuma módosította a 1332.38 direktíváját, és 8 év minimális katonai szolgálati időhöz kötötte az anyagi kompenzáció, és orvosi ellátás fizetésének lehetőségét a genetikai alapú, de a szolgálat kezdetekor még nem manifesztálódott betegségek kialakulása esetén [56d, 57b].

Az aktivált protein C (APC) rezisztenciát okozó Faktor V R506Q (FV Leiden) mutáció:

A mutáció miatt egy aktivált véralvadási faktor - az V. faktor - fehérjeláncát az aktivált protein C (APC) nevű enzim nem képes bontani. Az alvadást elősegítő faktorok bomlásának lassulása következtében az érintetteknek fokozottan alvadékony a vére, így trombózisra - azaz vérrögképződés okozta érelzáródásra - hajlamosak. A FV Leiden mutáció a vénás thrombosis bekövetkezésének valószínűségét heterozigóta (azaz egy mutáns és egy normál génhordozás esete) formában mintegy 7-szeresre, homozigóta formában 80-szorosra növeli.

A prothrombin G20210A mutáció jelentősége: A prothrombin a véralvadási kaszkádban központi szerepet betöltő, a fibrinogén-fibrin átalakulást katalizáló thrombin (II. faktor)

előalakja. A prothrombingén 3' nem transzlálódó régiójának pontmutációja következtében ugyan nem változik az átíródó fehérje szerkezete, viszont a keletkező prothrombin szintje kb. 30%-kal emelkedik. Ennek következtében fokozódik a véralvadási rendszer aktivitása, és nő mind a vénás, mind az artériás thrombózisra való hajlam.

*A metiléntetrahidrofolát reduktáz (MTHFR) enzim génjének pontmutációja (C677T):*A vér homocisztein-koncentrációjának emelkedése (hyperhomocysteinaemia) független tényezőként fokozza az ischémiás szívbetegségek, az agyi érbetegségek, a perifériás arteriosclerosis, a mélyvénás thrombózis kockázatát. Az MTHFR enzim C677T-es mutációja az enzim fokozott hőlabilitását eredményezi.

A cisztationin ß-szintáz (CBS) enzim génjének mutációja: A homocisztein-anyagcsere fontos enzimjének, egy gyakori, inszerciós mechanizmusú mutációja (844ins68) következtében alternatív intron-hasítási ("splice") hely keletkezik, és így a normálissal egyező méretű fehérje képződik. Az MTHFR C677T mutációjával kombinálódva fokozza a hyperhomocysteinaemia mértékét.

Ismert katonai biogenetikai eset: A prediktív katonai genetika egy másik alapesetének számít annak az amerikai hadseregben szolgáló helikopterpilóta nőnek az esete, akinek terhessége miatt – kímélete céljából – elrendelt irodai munkavégzése során mélyvénás alsóvégtagi rögösödése alakult ki, melynek hátterében, kivizsgálása után meglévő Leiden mutációjára derült fény. Genetikai öröksége miatt a katonaság leszerelte, további egészségügyi ellátásához nem járult hozzá, kártérítést részére nem fizetett. Bár később vizsgálóbíróság a katonaság részbeni felelősségét megállapította az egészségkárosodása, és felmentése hátterében, de a 2005 óta érvényben lévő USA Védelmi Minisztériumi Állásfoglalás alapján kártérítését megtagadták, mert az USA hadseregében csak 7 évet szolgált, szemben az utasítás által ilyen esetekben megkövetelt 8 éves minimális szolgálati jogviszony helyett (US Department of Defense Instruction 1332.38/2005 /E.3.P.4.5.2.2./ [56e, 57c].

KÖVETKEZTETÉSEK

A biotechnológiai XXI. századi eredményei és a HGP befejeződése megteremtették az alapját egy új tudományterület elkülönülésére, mely a *katonai biogenetika*. Ez jól körülhatárolható irányok mentén magába olvasztja számos humán és nem humán alap és alkalmazott biotechnológiai és genetikai kutatási terület eredményeit, melyek közül számosról úgy gondoltuk eddig csak a civil szférában hasznosulhat.

A már elérhető, és a bizonyosan megvalósítható alkalmazások szerves részét fogják képezni katonai stratégiák tervezésének, a katonai biogenetika eredményeinek használói feltétlen előnybe kerülnek a felderítés, a harckészség (humán erőforrás), az önvédelem, a katasztrófavédelem, a hatékony és effektív reagálás területén, és – a nemzetközi jog kereteit figyelembe véve – a nem halálos fegyverek tárházának bővülése következtében szinte a hadviselés minden szegmensében.

A katonai biogenetika teljes potenciáljának jogi és társadalmi elfogadtatása – túl az anyagi nehézségeken – azonban kétséges. Sokan (személyek, országok) vallási, erkölcsi, vagy etikai okokból alapvetően elleneznek minden próbálkozást, amely a növények, állatok és az ember genetikai állományának bármilyen fokú megváltoztatására és vagy használatára irányul. Civil szervezetek, és jogvédők ellenérvrendszerének szilárd alapja alapvetően az országok alkotmányaiban (törvényeiben, egyéb jogszabályaiban) vagy nemzetközi egyezményekben közvetlenül, vagy közvetetten rögzített *genetikai diszkrimináció, és katonai támadó célú felhasználás tilalma*.

Ezzel szemben a biogenetikában megengedőbb jogszabályi környezettel rendelkező országok, csoportok a genetikai forradalom érájában lépéselőnyre tehetnek szert az alap biogenetikai kutatási eredmények alkalmazhatóságának, kipróbálásának engedélyezésével, mind a civil mind a katonai szférában.

A katonai típusú alkalmazások tárházának bővülése pedig azok körében, akik életpályaként választják a katonaságot, egy másik következménnyel járhat. *A jövőben az ember, saját genetikai állományában rögzített információival való rendelkezésének joga, mely alapvetően a személy önrendelkezéséhez kötött jelenleg, sérülhet a katonai szolgálatba lépés pillanatában.*

Az előzőekben felvázoltak még hangsúlyosabban utalnak a katonai bioetika és a katonai biogenetika szoros kapcsolatára, továbbá a genetikai és a bioetikai tudás minél szélesebb körű terjesztésének szükségességére, beleértve természetesen a mindenkori graduális és postgarduális képzéseket, de a politikai és katonai döntéshozatali szinteket is.

A jelen publikációban csak felvázolni sikerült a katonai biogenetika néhány érdekes up to-date alkalmazási területét, és utaltunk a kérdéskör tágabb aspektusaira. A katonai biogenetikai tudásanyag hihetetlen gyorsütemű bővülése (és ezzel egyidejű gyors amortizációja!) miatt minden állampolgár tudásanyagának ilyen irányú bővítése szükséges, és része kell, hogy legyen a társadalmi, politikai, katonai felelős gondolkodásnak. Ez vezethet csak el ahhoz, hogy a civil, de különösen katonai területen megvalósuló bármely biotechnológiai és genetikai alkalmazás hasznosságáról, vagy elítéléséről, elvetéséről megalapozottan lehessen nyilatkozni.

A magyarországi hadtudományba megkezdődött a katonai biogenetika ismeretanyag beépülése, egyes elemei – a tömegpusztító, és a nem halálos fegyverek rendszerezésére vonatkozó fejezetekben – már megtalálhatók.

Nem ismert azonban az, hogy a hadtudomány előszobájában kopogtató biogenetikai forradalom milyen fogadó környezetet talál, milyen a katonai graduális és postgraduális képzésben résztvevők (leendő döntéshozók), oktatók, avagy a jelen katonai döntéshozóinak bioetikai-biogenetikai adaptációs ereje. Eddig, erről semmilyen felmérés sem készült. Ennek elvégzése sürgető, mert a közeljövő katonai stratégiai tervezése, vagy nemzetvédelmi koncepciók kialakítása, a kutatás-fejlesztési projektek prioritásainak kijelölése és az erre rendelkezésre álló anyagi erőforrások elosztása, ezen ismertek nélkül nem lehetséges [61,62].

A genomika /és biotechnológia/ töretlen, rapid fejlődéséből egyértelműen következik, hogy a katonai bio„genetikához való fordulás a következő leglogikusabb lépése a modern hadviselésnek” [63].

Irodalomjegyzék

[1] B. R. Jasny, D. Kennedy: The Human Genome. Science, 291 (2001) 1153.

[2] C. R. Darwin: On the origin of species by means of natural selection, or the preservation of favoured races in the struggle for life. (1861) London: John Murray. 3d edition.

[3] J. G. Mendel: Versuche über Pflanzen-Hybriden. Verhandlung des Naturforschenden Vereins in Brünn 4 (1866) 3-47.

[4] C. Correns: G. Mendel's Regel über das Verhalten der Nachkommenschaft der Rassenbastarde. Berichte der deutschen botanischen Gesellschaft, 18 (1900) 158–168.

[5] http://www.biodiversitylibrary.org/item/43179#page/5/mode/1up (2011.12.05)

[6] E. Tschermak: Über Künstliche Kreuzung bei Pisum sativum. Berichte der Deutsche Botanischen Gesellschaft, 18 (1900) 232-239.

[7] W. S. Sutton: On the morphology of the chromosome group in Brachystola magna. Biological Bulletin, 4 (1902) 24-39.

[8] http://www.jic.ac.uk/corporate/about/bateson.htm (2011.12.05)

[9] Gh. Hardy:. Mendelian proportions in a mixed population. Science 28 (706) (1908): 49–50. doi:10.1126/science.28.706.49. ISSN 0036-8075. PMID 17779291

[10] W. Weinberg: Über den Nachweis der Vererbung beim Menschen. Jahreshefte des Vereins für vaterländische Naturkunde in Württemberg, 64 (1908) 368–382.

[11] T. H Morgan: Chromosomes and heredity. The American Naturalist, 4 (1910) 449–496.

[12] A. H. Sturtevant: The linear arrangement of six sex-linked factors in Drosophila, as shown by their mode of association. Journal of Experimental Zoology, 14 (1913) 43-59.

[13] H. J. Müller: Artificial transmutation of the gene. Science, 46 (1927) 84-87.

[14] F. Griffith: The significance of pneumococcal types. Journal of Hygiene, 27 (1928) 113–159.

[15] G.W. Beadle, E.L.Tatum: The genetic control of biochemical reactions in Neurospora. Proceedings of the National Academy of Science, 27 (1941) 499-506.

[16] O.T. Avery, C.M. MacLeod, M. McCarty: Studies on the Chemical Nature of the Substance Inducing Transformation of Pneumococcal Types: Induction of Transformation by a Desoxyribonucleic acid Fraction Isolated from Pneumococcus Type III. Journal of Experimental Medicine, 79 (1944) 137-158.

[17] E. Chargaff: Chemical Specificity of Nucleic Acids and Mechanism of Their Enzymic Degradation. Experientia, 6 (1950) 201-209.

[18] J. D. Watson, F.H. Crick: Molecular structure of nucleic acids. A structure of deoxyribose nucleic acid. Nature, 171 (1950) 737–738, 964–967.

[19] J-H. Tjio, A. Levan: The chromosome number of man. Hereditas, 42 (1956) 1–6.

[20] F. H. C. Crick, L. Barnett, S. Brenner, R. J. Watts-Tobin R: General nature of the genetic code for proteins. Nature,192 (1961) 1227-1232.

[21] H. O. Smith, K. W Wilcox: A restriction enzyme from Haemophilus influenzae I. Purification and general properties. Journal of Molecular Biology, 51 (1970) 379-391.

[22] H. G. Khorana et al.: Total synthesis of the structural gene for the precursor of a tyrosine suppressor transfer RNA from Escherichia coli. 1. General introduction. J. Biol. Chem. 251 (1976) 565–570.

[23] A. M. Maxam, W. Gilbert: A new method for sequencing DNA. Proceedings of the National Academy of Science, 74 (2) (1977) 560–564.

[24] F. Sanger, S. Nicklen, A. R. Coulson: DNA sequencing with chain-terminating inhibitors. Proceedings of the National Academy of Science 74 (12) (1977) 5463–5467.

[25] K. Mullis et al.: Specific Enzymatic Amplification of DNA In Vitro: The Polymerase Chain Reaction. Cold Spring Harbor Symposium on Quantitative Biology, 51 (1986) 263.

[26] A. Monaco et al.: Isolation of candidate cDNAs for portions of the Duchenne muscular dystrophy gene. Nature, 323 (1986) 646-650.

[27] B. S. Kerem et al.: Identification of the cystic fibrosis gene: genetic analysis. Science,; 245 (1989) 1073-1080.

[28] R. D. Fleischmann et al.: Whole-genome random sequencing and assembly of Haemophilus influenzae. Science, 269 (1995) 496-512.

[29] The Genome International Sequencing Consortium: Initial sequencing and analysis of the human genome. Nature, 409 (2001) 860–941.

[30] J. C. Venter et al.: The Sequence of the Human Genome. Science, 291 (2001) 1341–1351.

[31] A. Serra: La rivoluzione genomica: La Civiltà Cattolica, 152 (2001) 439–453.

[32] http://www.insurancejournal.com/news/international/2011/02/03/183171.htm, (2011.06.21.)

[33] http://operatingexperience.doe-hss.wikispaces.net/file/view/Department+of+Commerce+Counterfeit+Electronics+Report.pdf (2011.06.21.)

[34] http://dcg.materials.drexel.edu/wp-content/publications/JApplPhys_Vol91_Num10_2.pdf, (2011.06.21.)

[35] http://www.adnas.com/, (2011.06.21.)

[36] http://www.pr-inside.com/print1253362.htm, (2011.06.21.)

[37] http://www.adnas.com/sites/default/files/apdn_marks_microchips_for_dod_june_22_2011.pdf, (2011.06.21.)

[38] http://www.opbw.org, (2011.05.28)

[39] http://www.cbd.int/biosafety/, (2011.05.28)

[40] A. Juhaz, R. Naidu: Bioremediation of high molecular weight polycyclic aromatic hydrocarbons: a review of the microbial degradation of benzo [a]pyrene. International Biodeterioration and Biodegradation, 45 (2000) 57-88.

[41] A. Thomas, E. Hill: Aspergillus fumigatus and Supersonic Aviation. International Biodeterioration and Biodegradation, 48 (2001) 245-251.

[42] J. D. Gu et al.: Microbial degradation of polymeric coatings measured by electrochemical impedance spectroscopy. Biodegradation, 1 (1998) 39-45.

[43] D. Nica et al.: Isolation and characterization of microorganisms involved in the biodeterioration of concrete in sewers. International Biodeterioration and Biodegradation, 46 (2000) 61-68

[44] G. P. Brahmaprakash et al.: Development of Thiobacillus ferrooxidans ATCC 19859 strains tolerant to copper and zinc. Bulletin of Materials Science, 10 (5) (1988) 461-465.

[45] G. Sayler: Field applications of genetically engineered microorganisms for bioremediation processes. Current Opinion in Biotechnology, 11 (2000) 286-289.

[46] T. J. Fleischmann et al.: Anaerobic transformation of 2,4,6-TNT by bovine ruminal microbes. Biochemical and Biophysical Research Communications, 314, 4 (2004) 957-963.

[47] A.M. Chakrabarty: Microorganisms having multiple compatible degradative energy-generating plasmids and preparation thereof. United States Patent, 4259444 31.03.1980.

[48] H. J. Agostini et al.: Identification and characterization of uvrA, a DNA repair gene of Deinococcus radiodurans. J. Bacteriol, 178 (1996) 6759–6765.

[49] T. Zwillich: A tentative comeback for bioremediation. Science, 289, 5488 (2000) 2266-2267.

[50] J. D. Gu et al.: Microbial degradation of materials: general processes. In: Revie, W. (ed.) The Uhlig Corrosion Handbook (2nd ed.), John Wiley & Sons, New York, 349 – 365. (2000)

[51] P. Szafranski, Ch. Mello, T. Sano: Compositions and methods for controlling genetically engineered organisms. (US Patent 6287844) 09.11.2001.

[52] J. von Aken, E. Hammond: Genetic engineering and biological weapons. EMBO reports (special issue), 4 (2003) 57-60.

[53] L. Juhász., A. Huszár: Gondolatok Ken Alibek: Biohalál című könyve kapcsán http://www.edis.hu/?pageid=tudastar_biohalal, (2001). (2010-09-22)

[54] Genetic Information Nondiscrimination Act: USA, Public Law (2008) 110-233, 122 Stat. 881 (érvényben 2008.május 21-től)

[55] P. A. Ham: An army of suspects: The history and constitutionality of the U.S. military's DNA repository and its access for law enforcement purposes. Army Lawyer, 2003 July/August (2003) 1-19.

[56] S. Baruch, K. Hudson: Civilian and military genetics: Nondiscrimination policy in a Post-GINA World. AJHG, 83 (2008) 435-444.

[57] M. Nunes: Public remarks at Genetics and Public Policy Center conference Washington, DC., http://www.dnapolicy.org/news.past.php?action=detail&past_event_id=25, (2006). (2011.07.01.)

[58] P.B. Gold, B. Frueh, B. Christopher: Compensation-seeking and extreme exaggeration of psychopathology among combat veterans evaluated for posttraumatic stress disorder. Journal of Nervous & Mental diseases, 187 (11) (1999) 680-684.

[59] Committee on Veterans Compensation for Posttraumatic Stress Disorder, Institute of Medicine and National Research Council: PTSD Compensation and Military Service. The National Academies Press, ISBN-10: 0-309-10552-8 (2007).

[60] J.M. Wolf, S. Mountcastle, B. D. Owens: Incidence of Carpal Tunnel Syndrome in the US Military Population. Hand, 4,4 (2007) 289-293

[61] A. Huszár: A bioetika katonai vonatkozásai és a nem halálos fegyverek. http://www.zmne.hu/tanszekek/ehc/konferencia/april2001/eload2.html, (2001). (2011.06.30.)

[62] I. Resperger: Kockázatok, kihívások és fenyegetések a XXI. században. Az Országos Kiemelt Kutatási Tanulmányok pályázata, (2002) 24.

[63] R. Christopher: Genesis – The apocalypte. ISBN-10: 1424160227 (In USA 09.30/2007) http://www.prweb.com/releases/2007/12/prweb576709.htm, (2011.06.30.)

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Pápai Tibor
tibor.papai@gmail.com

A HARCTÉRI ELSŐSEGÉLYNYÚJTÁS HELYE A HADSZÍNTÉRI ELLÁTÁSBAN ÉS ANNAK OKTATÁS MÓDSZERTANI IRÁNYVONALAI

Absztrakt

Magyar Honvédség széleskörű feladatrendszere miatt az elsősegélynyújtás és a harctéri elsősegélynyújtás készségszintű alkalmazása végzettségtől, beosztástól, rendfokozattól függetlenül minden katonára egységesen vonatkozik, ezért az elsősegélynyújtás és a harctéri elsősegélynyújtás kompetencia szintű alkalmazása valamennyi katonától elvárt képesség kell, legyen! A harctéri sérülések kimeneti mutatóinak javítása érdekében, döntő szerepe van a sérülés - kimentés - segélynyújtás – emeltszintű ellátás láncnak. Ebben a mentési láncban foglal fontos helyet a harctéri elsősegélynyújtó.

The application of first aid based on skills -qualification-position, regardless of rank applies to every soldier, because of the wide range of tasks of the Hungarian Army; therefore the battlefield first aid and so first aid are required from each soldier on a competence level. In order to improve the output characteristics of battlefield injuries there is a decisive role of damage-rescue assistance and high level supply chain. In this free chain battlefield first aid first aid takes an important place.

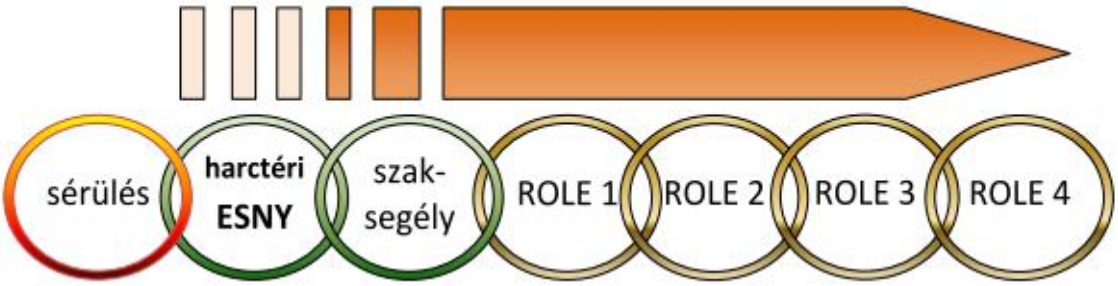
Kulcsszavak: *elsősegélynyújtás, harctéri elsősegélynyújtás, minősített állapot, kompetencia, képesség, oktatás, módszertan ~ first aid, battlefield first aid, certified status, competence, skills, training, methodology*

AZ ELSŐSEGÉLYNYÚJTÁS, HARCTÉRI ELSŐSEGÉLYNYÚJTÁS FEJLŐDÉSÉNEK RÖVID TÖRTÉNETE

Az önzetlen segítségnyújtás iránti vágy az ember egyik legrégebbi késztetése. A segítségnyújtás célja minden időben ugyanaz volt: a sérült ember életének megmentése, fájdalmának, szenvedésének csökkentése egészségének mielőbbi visszaadása érdekében. A fennmaradt régészeti leletek is bizonyítják a segélynyújtás korai, kezdetleges, de hatékony módszereinek folyamatos fejlődését, mely fejlődést még napjainkban sem tekinthetjük befejezettnek. A fejlődés állomásainak tanulmányozása alapján elmondható, hogy napjainkban, a polgári életben elsősegélynyújtásként nevezett tevékenység fejlődésében jelentős szerepe volt a harctéren alkalmazott segélynyújtási technikáknak. Elsősegélynyújtást bizonyító leleteket találtak az ókori görög, római régészeti feltárások során is. Ezek az ókori katonaállamok nagy hangsúlyt fektettek a sebesült katonák harctéri ellátására és ápolására az ismételt mielőbbi hadrafoghatóság érdekében. A kereszténység elterjedésével virágzott fel a kolostori medicina. A bajbajutottak megsegítését már szervezettebb formában végezték a Johanniták által 967-ben alapított Bernáthegyi kolostor lakói. A rend lovagokat képzett a harctéri sérültek ellátására. Ebben a korban a keresztes hadjáratok eredményeként jöttek létre a szerzetesrendek, hadi ápolórendek és lovagrendek, amelyek a sebesültellátást biztosították a Szentföld felszabadításáért harcolóknak. Magyarországon az elsősegélynyújtási kötelezettség régóta törvényileg szabályozott. Elsőként Mária Terézia 1769-ben kiadott „Rendelet a rögtöni segélynyújtásról” rendelete szabályozta a Birodalom területén az elsősegélynyújtást.[1] 1859 az osztrák- olasz-francia háború éve, egymást követik a véresebbnél véresebb ütközetek. Június 24-én a solferinoi ütközet borzalmai nyomán Henry Dunant felismerte, hogy az osztrák és francia áldozatok jelentős része azon sebesült katonák közül került ki, akik nem jutottak időben megfelelő elsősegélyhez. Az első világháborúban a magyar szanitécek nadrágszíjukban egy nagyméretű biztosítótűt hordtak, melyet az eszméletlen fejsérült katonák légútjainak biztosításához használtak. A légutak megnyitására szolgáló műfogás (fej hátrahajtása, nyelv előrehúzása) után a sérült nyelvét az alkohollal vagy gyertyalánggal lefertőtlenített biztosítótűvel átszúrták. Így a nyelv nem tudott hátracsúszni a gégefedőre és kivédték a sérült fulladásos halálát. A második világháborúban a harctéren szolgálatot ellátó brit ápolók ideiglenes vérzéscsillapítás, fertőzés elleni védelem és fájdalomcsillapítás céljából a vérző sebszéleket pillanatragasztóval egyesítették. E rövid áttekintésből kiderül, hogy amíg az elsősegélynyújtás évezredek alatt a legősibb formájától a mai modern formájáig eljutott, sok ember munkájára, tapasztalatára, tudományos kutatására és megfelelő oktatásmódszertan alkalmazására volt szükség. A törvényalkotók napjainkban is fontosnak tartják a segítségnyújtás törvényen belüli szabályozását. A jelenleg hatályban lévő 1997. évi CLIV. törvény az egészségügyről, az 5. § e. pontjában kitér a mindenkitől elvárható segítségnyújtásra, és a VI. fejezet 125. § külön tárgyalja az egészségügyi dolgozókra vonatkozó jogi előírásokat. A segítségnyújtás elmulasztása jelenleg is büntetendő cselekmény és a Büntető Törvénykönyv 1978. évi IV. tv. 172. § (1) szankcionálja. Két év szabadságvesztést, vagy pénzbüntetést ró arra, aki a szükséges segélynyújtást elmulasztja. Három évre növekszik a büntetési tétel, ha mulasztás miatt az áldozat meghal. A közhiedelemmel ellentétben fontos megemlíteni, hogy a hazai szabályozásban nem található paragrafus a hibás segélynyújtás jogi szankcionálására.[2] A „jó szamaritánus” elv érvényesül és feltételezik, hogy aki bajbajutott társán önzetlenül segít, azt jó szándékkal teszi. A törvényi szabályozások és a sürgősségi ellátás folyamatán belül az elsősegélynyújtásban végbemenő szemléletbeli, szakmai és technikai változások, átszervezések hatására az elsősegélynyújtás oktatása egyre nagyobb hangsúlyt kap, egyre szélesebb körben zajlik.

AZ ELSŐSEGÉLYNYÚJTÁS, HARCTÉRI ELSŐSEGÉLYNYÚJTÁS HELYE, SZEREPE

Rohanó világunk mindennapjaiban mindannyian lehetünk áldozatok és segítségnyújtók, így az elsősegélynyújtás szükségére nem csak háborús és minősített időszakokban kerülhet sor, hanem békeidőben is. Fontosnak tartom megjegyezni, hogy bármilyen időszakban kerül sor az elsősegélynyújtás szükségére, az ellátás szakmai irányelvei nem változhatnak. Az elsősegélynyújtás azon ismeretek közé tartozik, amelyet mindenkinek el kellene sajátítania, a bajbajutott embertárs megmentése céljából. Elsősegélynyújtásra a legváratlanabb időben, a legváltozatosabb helyszínen és körülmények között kerül sor. Az elsősegélynyújtás lehetőséget ad arra, hogy az áldozatok még a szaksegítség megérkezése előtt segítséget kapjanak embertársaiktól. Az elsősegélynyújtó gyakran csak saját tudására, eszközök hiányában ötletességére hagyatkozhat, ezért fontos, hogy azokat a beavatkozásokat sajátítsuk el, amelyeket ilyen körülmények között minimális eszközökkel, vagy eszközök nélkül is jól tudunk alkalmazni. A helyszínen a sürgősségi ellátásban jártas szakember is csak ezeket a beavatkozásokat, tudja elvégezni, ha nincs birtokában életmentő eszköz, gyógyszer. A társadalom elvárása az, hogy minden időszakban minél több állampolgár legyen képes szakszerű és sikeres elsősegélyt nyújtani. A békeidőben kialakuló sérülések és a különböző jellegű megbetegedések következtében létrejövő egészségkárosodások (hirtelen halál, szívinfarktus, agyi vérellátási zavar stb.) évről évre emelkedő tendenciát mutatnak hazánkban is. A statisztikai adatok azt mutatják, hogy a balesetek, hirtelen fellépő megbetegedések előfordulási százaléka igen nagy, melynek okaként több tényező (technikai fejlődés, egészségi állapot romlása, társas kapcsolatok romlása stb.) említendő. A békeidőre vonatkozó rossz prognózisú mutatók a Magyar Honvédség állományát is ugyanolyan arányban érintik, mint a polgári lakosságot, amikor szükséges lehet a jelenlévők elsősegélynyújtási képességeinek bevetése. Ezen felül fontos kiemelni, hogy a Magyar Honvédségben, mint „veszélyes üzemben” a békeidőben történő speciális kiképzési és felkészítési feladatok (lőgyakorlatok, robbantási gyakorlatok, vegyi gyakorlatok, terep gyakorlatok, testnevelési foglalkozások, stb.) ellátása közben is szükség lehet elsősegélynyújtásra, azonban ilyenkor gyakran már nem elegendő a „polgári elsősegélynyújtás” készség szintű alkalmazása. Hazai viszonylatban az egyre gyakrabban előforduló, különböző nagyságú és súlyosságú minősített helyzetekben, (pl. katasztrófa, árvízvédelem stb.) a helyszíni ellátás során már szükség lehet speciális katona egészségügyi (ABV ismeretek, ellátásszervezés minősített helyzetekben) és harctéri elsősegélynyújtási (speciális kimentések, biztonsági zóna kialakítása, vérzéscsillapítás) ismeretekre is. Végül, de nem utolsó sorban a Magyar Honvédség külföldi missziós szerepvállalásai miatt a harctéri elsősegélynyújtás készségszintű alkalmazása elengedhetetlen az állomány részére. Ezen tényszerű érveken túl utalnék az előzőekben már leírt társadalmi elvárásra, miszerint minden időszakban minél több állampolgár legyen képes szakszerű és sikeres elsősegélyt nyújtani. Ez a társadalmi elvárás hatványozottan érinti az „egyenruhások” körét, hiszen a katona mindig, minden körülmények közt nyújtson segítséget a rászorulóknak! Ez a hatványozott segítségnyújtási kötelezettség végzettségtől, beosztástól, rendfokozattól függetlenül minden katonára egységesen vonatkozik, ezért az elsősegélynyújtás és a harctéri elsősegélynyújtás kompetencia szintű alkalmazása valamennyi katonától elvárt képesség kell, legyen! Ezen elvárások és képességek egységesítése céljából a katonák harctéri egészségügyi ellátása a NATO hadseregeiben szabályozottan történik.

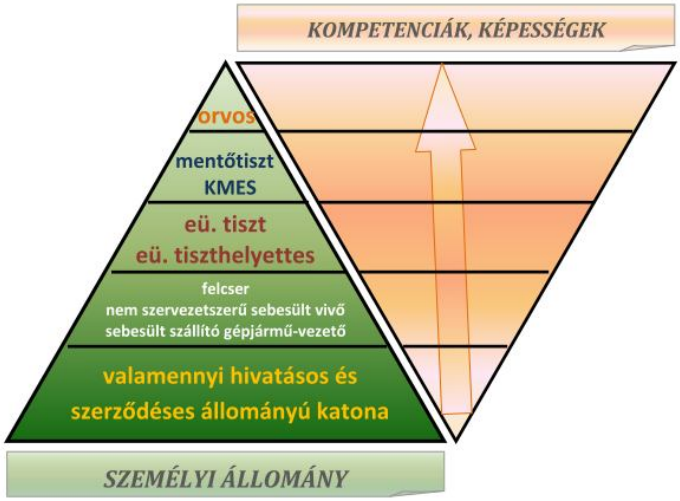


1. ábra. A harctéri elsősegélynyújtás helye a sérültellátás folyamatában (saját ábra)

A harctéri ellátás során a szakaszos sérült ellátás elveit kell követni, ami azt jelenti, hogy minden sérült katonát ott látnak el, ahol a sérülés súlyossága alapján szükséges. Ennek a szakaszos harctéri ellátásnak az első fázisa a harctéri elsősegélynyújtás, amit a katonák bajtársi segélynyújtás elve alapján egymásnak nyújtanak az ön és kölcsönös segélynyújtáshoz rendszeresített egységes sebkötöző csomagjuk használatával. A második szint már a szaksegély, amit már a peremvonaltól nem messze egy védett biztonságos helyen kialakított „sebesültgyűjtő fészekben" nyújtanak, a harctéren elsősegélyben részesített és oda vitt sérült katona részére. Itt általában egy magasabb képzettséggel és eszközökkel rendelkező egészségügyi katona látja el a sérülteket, mind addig, amíg a következő ellátási szintre nem transzportálják a sérültet. A következő szinteken már nem elsősegélynyújtás szintű ellátás folyik. Ezek az első orvosi segélyhely (ROLE 1) majd az első tábori kórház (ROLE 2) ez után a civil vagy katonai kórházi ellátás (ROLE 3) és szükség esetén a hátországban található kórház (ROLE 4). [3]

A harctéri elsősegélynyújtási képesség hatékonyságának megtartásához nem lehet figyelmen kívül hagyni a XXI. századi hadviselés főbb specialitásait, melyek jelentős mértékben befolyásolják az ellátási taktikák alakulását, annak módosításának szükségességét. A haditechnika fejlődése miatt újabb, súlyos sérülési mechanizmusok megjelenése, az ellátási szintek közti jelentős távolságok, az emeltszintű beavatkozások korlátozott hozzáférhetősége és a sérült evakuáció elhúzódása miatt egyre nagyobb az igény speciálisan képzett, megfelelő képességekkel és felszereléssel rendelkező állományra.

A változó ellátási koncepciók és a sikeresen ellátott sérültek számának növelése céljából egy új típusú képzés is bevezetésre került a NATO és ma már a Magyar Honvédség állományában is. A harctéri életmentő katona - Combat Life Saver, (egy készülő HM rendeletben KMES – különleges műveleti egészségügyi katona elnevezéssel tervezve) az a katona, aki polgári egészségügyi képesítéssel nem rendelkezik, de a NATO és az MH által szervezett egészségügyi szakkiképzést sikeresen elvégezte és katonai feladatainak ellátása közben hadműveleti területen és Magyarországon a katonai feladat ellátása közben, ha harci feladatai megengedik másodlagos tevékenységként a sérültet a rendeletben megfogalmazott kompetenciái szerinti ellátja. Főbb tevékenységei lehetnek a sérült vizsgálata, emelt szinten vérzéscsillapítás, törés ellátás, égési sérülés ellátása, eszközös légútbiztosítás kivitelezése, folyadékpótlás intravénás, szükség esetén intraosseális kanülálással, mellkasi sérült emeltszintű ellátása (detenzionálás). [4]



2. ábra. Kompetenciák alakulása a harctéri sérültellátás során
(saját ábra)

Fontos, megjegyezni, hogy a harctéri sérültellátást emeltebb szinteken végző állomány megjelenése az ellátó rendszerben nem jelenti az elsősegélynyújtás, harctéri elsősegélynyújtás jelentőségének, fontosságának csökkenését! Az elsősegélynyújtás, harctéri elsősegélynyújtás képességeinek minél szélesebb körben, minél korszerűbb módszerekkel történő oktatása elengedhetetlen az érintett célcsoport számára. Publikációm célja, hogy a Magyar Honvédség valamennyi hivatásos és szerződéses állományú katonája számára hangsúlyozni a képesség szintjén végzett elsősegélynyújtás és harctéri elsősegélynyújtás fontosságát, valamint ennek oktatásához szakmai hátteret nyújtani a minőség, kontrollálhatóság, számonkérés és az elsajátított képességek szinten tartása végett.

AZ ELSŐSEGÉLYNYÚJTÁS KOMPETENCIÁI

Az alábbi táblázat az egészségügyi szakképzésben az Első ellátás- elsősegélynyújtás alapmodul elvégzése során megszerezhető kompetenciákat tartalmazza, amely kompetencia valamennyi képzett elsősegélynyújtóra vonatkozik!

A helyszín biztonságosságát felméri	Az elsődleges beavatkozásokat megkezdi/elvégzi: o zavart tudatú betegnél, o fájdalomról panaszkodó betegnél, o nehézlégzéssel küszködő beteg esetén, o görcsroham alatt és után, o beszédzavar, végtaggyengeség esetén, o sokkos állapotú betegnél, o mérgezés gyanúja esetén, o elektromos balesetet szenvedett betegnél.
A helyszíni körülményekről tájékozódik	
Tájékozódó állapotfelmérést végez	
A figyelemfelhívó panaszokat/tüneteket felismeri	
Segítséget hív	
A beteget állapotának megfelelő testhelyzetbe hozza	
Halaszthatatlan beavatkozásokat végez	
Újraélesztést végez	
Eszméletlen betegnél eszközzel és eszköz nélkül légutat biztosít	

Vérzéscsillapítási eljárást alkalmaz	Tömeges baleset felszámolásában segédkezik
Hőhatás okozta sérülést ellát	Katasztrófa-egészségügyi ellátásban közreműködik
Elsődleges sebellátást végez	Beteget mozgat, műfogásokat alkalmaz
Kötözéseket alkalmaz	A beteg szállításra történő előkészítésében segédkezik
Rándulásokat, ficamokat, töréseket rögzít	

1. táblázat. A képzett elsősegélynyújtó kompetenciái békeidőben [5]

A HARCTÉRI ELSŐSEGÉLYNYÚJTÁS SPECIALITÁSAI

A fegyveres konfliktusokban részt vevő felek egészségügyi veszteségeiben a legfontosabb szerepet játszó tényezők, a résztvevő fegyveres alakulatok közti erőviszony, az alkalmazott fegyverfajták, az alakulatok állományának fizikai és pszichikai felkészítettsége, kiképzettsége, valamint az egészségügyi ellátás szakmai és technikai színvonala. A technika, fegyveripar fejlődésével párhuzamosan a sérülések jellege, és a súlyos sérültek aránya is változik. A sérültek letalitásának csökkentése érdekében, döntő szerepe van a sérülés - kimentés - segélynyújtás folyamat időablakoknak, a magas szintű, jól szervezett segélynyújtásnak, az ellátott sérültek megfelelő transzportjának, a sérült állapotának és ellátási igényének megfelelő szintű ellátó helyre.

A békeidőben alkalmazandó elsősegélynyújtás kompetenciáit a harctéri elsősegélynyújtás során speciális képességekkel szükséges bővíteni. A sürgősségi helyzetek generálta stressz régóta ismert jelenség. A sérülés látványa, a sérült szenvedése, a közvetlen rokoni, baráti, bajtársi viszony esetén a bizonytalannak gondolt elsősegélynyújtó készség, a fokozott félelem az elvesztéstől súlyos deprimáló feszültséget válthat ki a segélynyújtóban. A stressz keltette pszichológiai folyamatok eldöntik, eldönthetik, hogy adott esetben a segélynyújtó képes lesz-e beavatkozásra, vagy nem. A harctéri sérült ellátás során ezek a tényezők kiemelt jelentőséggel bírnak a szituáció, a veszélyes környezet, az aránytalanul sok sérült száma miatt. A segélynyújtás közben vagy után jelentkező úgy nevezett „post traumatic stress" megelőzésének tárgyalása a tematika része kell, hogy legyen. Az elsősegély gyakorlatok során fel kell készíteni a segélynyújtót a harctéri helyzetekben jelentkező stressz faktorokra. A segélynyújtás után esetleg panaszokat okozó stressz felismerésére (szorongás, alvászavarok, ingerlékenység), valamint fel kell hívni a figyelmet annak feloldásának lehetséges módjára.

A harctéri sérültellátás során minden elsősegélynyújtó tevékenység (kimentés, újraélesztés, légútbiztosítás, sérülésellátás stb.) megkezdésének fontos feltétele a biztonságos ellátás körülményeinek megteremtése, fedezék keresése, rejtőzködés, egyébként ettől eltérő esetben a segélynyújtó is az esemény áldozatává válhat. Ezért kell elsajátítani a gyors helyzetfelismerést és felmérést, a helyszín biztonságos megközelítését és a biztonságos környezet kialakítását, a sérültek elsődleges vizsgálatát és állapotfelmérését, az ellátási prioritás felállításának (triage) módszerét és a helyszíni ellátás menetét, taktikáit. A sérült biztonságos környezetbe szállításához speciális kimentési eljárásokat kell alkalmazni, amelyhez nem elegendő, és a speciális felszerelés miatt nem is kivitelezhető a sérült kimentésére szolgáló Rautek- féle műfogás. Speciális kimentési műfogásokat, praktikumokat kell alkalmazni a lövészárokból,

harci járműből, tűztérből való mentés során. Ezért is fontos a képességek gyakorlását a valós helyzetekhez legjobban hasonlító körülmények között gyakorolni. [3]

A harctéri sérült ellátás során leggyakrabban előforduló speciális sérülések is módosíthatják az elsősegélynyújtás kompetenciáját. A leggyakrabban előforduló baleseti mechanizmusok a lőtt, robbantott sérülések, lövedék, repesz okozta sérülések, égési sérülés, épületomlás miatt betemetés, magasból esés, és nagy sebességű gépjármű, harci jármű balesete lehet.

A nyílt terepen keletkezett sérülések főbb jellemzői a lágyrész sérülések, nyílt és szilánkos csonttörések, valamint zárt végtag és koponyasérülések. Zárt helyen (épületben, gépjárműben) történő sérüléskor tompa traumák, zárt végtagtörések, koponya és csigolyatörések, továbbá belső szervek morfológiai, funkcionális károsodásainak változatos formái jelennek meg. Robbanáskor a keletkező hő és láng okozta égési sérülések, valamint a gáztermékek általi toxikus ártalmak teszik speciálissá a segélynyújtás és ellátás folyamatát.[6] Ezen sérülések miatti halálozást az életfontosságú szervek és végtagok roncsolódása, a heveny vérveszteség és annak következményeként kialakult sokk, légúti elzáródás és feszülő légmell miatt kialakult légzési elégtelenség okozza. A harctéri halálozások közel 90 %-a a sérült ellátó helyre érkezése előtt következik be. A halálesetek oka az első 10 percben az életfontosságú szerv, szervek nagyfokú roncsolódása, 2-3 órán belül a nagyfokú vérveszteség, 4-12 órán belül a sokk miatti szervi elégtelenség lehet. Szakirodalmi adatok alátámasztják, hogy az idejekorán elkezdett elsősegélynyújtással, a sérültek kiszállítási időtartamának optimalizálásával és az első szakszerű sürgősségi segély működtetésével a harctéri primer halálozás jelentősen csökkenthető, így a kórházat élve elérő súlyos sérültek aránya lényegesen jobb. Az optimális kimeneti mutatók megtartásához elengedhetetlen a sérülés és az első ellátás közti időtartam csökkentése, az első szaksegély és sürgősségi segély szintjének emelése, és a sürgősségi sebészeti jellegű beavatkozások optimális esetben 1 órán, de legalább 6 órán belüli elvégzése. Tanulmányok rámutattak arra, hogy a potenciálisan kivédhető, menthető harctéri halálozás 35-37 %-os lehet, ebből 15% csak az idejekorán elkezdett, szakszerű bajtársi elsősegély révén valósulhat meg. Ilyen jellegű sérülésekkel a katonák gyakran találkozhatnak elsősorban békefenntartó missziókban (KFOR, ISAF), de szembesülhetnek hasonló mechanizmusú sérüléssel békeidőben is, különböző ipari jellegű robbantások, visszamaradt nem hatástalanított háborús robbanószerkezetek, vagy különböző terrorcselekmény, alvilági leszámolás során. Ezért kiemelt jelentőséggel kell kezelni, hogy a harctéri segélynyújtás során a katonák képesek legyenek a mielőbbi fedezék feltalálására és szükség esetén rejtőzködésre, a rendszeresített egyéni egészségügyi felszerelésük (nyomókötés, tourniquet) alkalmazásával mielőbbi hatékony vérzéscsillapításra.

AZ ELSŐSEGÉLYNYÚJTÁS, HARCTÉRI ELSŐSEGÉLYNYÚJTÁS OKTATÁSÁNAK MÓDSZERTANI SZEMPONTJAI

Az elsősegélynyújtás, harctéri elsősegélynyújtás minőségi oktatásának szervezéséhez fontos meghatározni a szükséges személyi és tárgyi feltételeket, az alkalmazandó oktatási tematikát, az oktatásmódszertant és az elsajátított ismeretek mérésének módszertanát, annak értékelési szempontjait.

Az oktatók személyének kiválasztásánál minimum feltétel az aktuális nemzetközi és hazai irányelvek, szakmai ajánlások és azok hátterének elméleti és gyakorlati ismeretén túl a megfelelő, (elsősorban harctéri ellátásban szerzett) szakmai tapasztalat és oktatói gyakorlat. Bizonyos képességek oktatásához fontos követni a nemzetközi ajánlásokat, így például az újraélesztés oktatásához elvárás az oktató személyétől, hogy az Európai Újraélesztési Társaság (ERC) akkreditált oktatója (BLS/AED instructor) legyen.[7] Fontos megjegyezni,

hogy az oktatói feladat ellátását nem kell orvosi végzettséghez kötni. Célszerű vegyes oktatói csoportokat kijelölni, amelyben a minimum feltételeknek megfelelő más egészségügyi végzettségű szakdolgozók (mentőtiszt, diplomás ápolók, szakápolók) is részt vehetek. A minőségi oktatás biztosítása szempontjából kiemelten kell kezelni az oktatók ismereteinek fejlesztését, szinten tartását, és az új, akár szakmai, akár módszertani koncepciók és praktikumok mielőbbi átadását.

A személyi feltételeknél az oktatói képességek és feltételek szabályozásán túl a gyakorlati képzés hatékonyságának megtartása céljából meg kell határozni az oktatók/ hallgatók arányát a gyakorlati foglalkozásokon. A gyakorlati foglalkozásokon minden hallgató részére biztosítani kell, hogy az előírt gyakorlatot az elvárt készség szintjén tudja elsajátítani, ezért a nemzetközi ajánlások alapján az ilyen foglalkozások során törekedni kell a kiscsoportos, maximum 8 fős létszám kialakítására, de harctéri szituációs gyakorlatok során a 6 fős csoport javasolt.

A személyi feltételek szabályozásán túl fontos megemlíteni a hatékony oktatás biztosításához szükséges tárgyi feltételek meglétét. Az elméleti és gyakorlati foglalkozásokhoz megfelelő kubatúra kell rendelkezésre álljon. Kiemelt jelentőségű a harctéri elsősegélynyújtás gyakorlati oktatásához a valódi szituációhoz a lehető legjobban hasonlító környezet (pl. harctéri körülmények, gépjármű technika, rendszeresített eszközök stb.) kialakítása, biztosítása.

Ezen elvárások biztosítása céljából fontos kidolgozni a tananyagfejlesztés módszertana (DACUM, Brain storming technikák alkalmazása, feladat profilok és vizsgakövetelmények meghatározása stb.) szerint egy a nemzetközi, NATO és hazai szakmai irányelveknek megfelelő egységes tananyagtartalmat, kompetencia listát, oktatás módszertani ajánlást. A képzési program kialakítása során meg kell határozni a képzés formáját amely, lehet különböző (MSc, BSc, középiskolai) szintű, különböző formájú (nappali, levelező, esti, távoktatás jellegű) iskolarendszerű képzés és iskolarendszeren kívül szervezett tanfolyami jellegű vagy más tanfolyamba beintegrált jellegű képzés. Fontos megjegyezni, hogy a képzés szintjétől, formájától, jellegétől és az abból adódó eltérő óraszámoktól függetlenül a képzés végén a kimeneti kompetenciák és készségek egységesek kell, hogy legyenek.

Az elsősegély oktatásának módszertana hatalmas fejlődésen ment keresztül az elmúlt években. A helyes oktatásmódszertant a célcsoport életkora, esetleges előzetes ismeretei, szakirányú végzettsége, motiváltsága alapján kell megválasztani. Az elméleti oktatások során nagy hangsúlyt kell fektetni az oktatónak a hallgatók megfelelő figyelemfelkeltésére, motiválására és a foglalkozásokon való aktív bevonására. Ehhez az oktatónak pedagógiai, didaktikai, módszertani, oktatástechnológiai ismerettel kell rendelkezni. Felnőttek képzése során elengedhetetlen az andragógiai ismeretek alkalmazása. A képzés sikerét, hatékonyságát, és a megfelelő dinamikájú haladást segíti elő, ha a hallgatók az elméleti ismeretek tananyagát a képzés indulása előtt 2 héttel előre megkapják tanulmányozás céljából. Heterogén összetételű csoportok esetében a helyes oktatásmódszertan és a képzés dinamikájának, struktúrájának helyes maghatározását segítheti, a hallgatók ismereteinek bemeneti mérése. Amennyiben a minőségirányítás elkötelezettjei vagyunk, a bementi felmérés a képzés hatékonyságának meghatározását is szolgálhatja, ha a képzés befejeztével összehasonlító jelleggel ugyanolyan mérést végzünk.

Az egységes oktatási tematika kialakítása során fontos szempont a megfogalmazott képességek eléréséhez szükséges óraszám meghatározásán túl az elmélet- gyakorlat arányának meghatározása. Tekintettel mind az oktatói, mind a hallgatói oldal (főként a munka melletti képzés során) jelenlegi globálisnak mondható humánerőforrás problémáira az óraszámok meghatározásánál a valóban szükséges óraszámot kell meghatározni. A túl hosszú képzések, tanfolyamok nem emelik az elvárt képességek hatékonyságát, de sokkal nagyobb a

költségvonzatuk (oktató részéről óradíj, hallgató részéről az eredeti feladat ellátásából kieső munkaidő). Az elmélet-gyakorlat aránya optimálisan 50%-os, de tekintettel, hogy a célunk elsősorban képességek és készségek (skillek) lehető legmagasabb szintű elérése, ebben az esetben ez az arány a gyakorlat javára eltolva 70 % -ban az optimális, amely a képzés hatékonyságának emelkedését szolgálja. A gyakorlatok legfőbb célja a skillek megfelelő elsajátítása után, azokat megfelelő scenariokba építve, a hallgató az adott körülményekhez, valós eszközökkel megfelelően adaptálja. A kimenet egységesítése céljából fontos, hogy a gyakorlatok lehetőleg egységes skillek és scenariok szerint legyenek szervezve.[8] Javasolt a skillek átadására az úgynevezett *négylépcsős módszer* alkalmazása az alábbiak szerint.

- *első lépcső*: a gyakorlatot bemutatja az oktató
- *második lépcső*: a gyakorlatot magyarázattal mutatja be az oktató, a bemutató során elmagyarázza az ok-okozati összefüggéseket, majd lehetőséget biztosít a résztvevők számára a bemutatott gyakorlattal kapcsolatban kérdés feltételére.
- *harmadik lépcső*: a hallgatók köréből véletlenszerűen kiválasztott résztvevő magyarázata alapján mutatja be a gyakorlatot az oktató
- *negyedik lépcső*: a hallgató önállóan végzi el a gyakorlatot, szükség esetén az oktató korrigálja az esetleges hibákat, majd a gyakorlat befejeztével értékeli a hallgató teljesítményét. [7]

Az egységes oktatási tematikán túl fontos az egységes kimeneti feltételek meghatározása. Meg kell határozni az elsajátított ismeretek mérésének módját, mely jelen esetben írásbeli és gyakorlati vizsgával történjen. Az írásbeli vizsga az elsajátított elméleti ismeretek és az ok-okozati összefüggések felmérését szolgálja. Az egységes kimenet céljából célszerű a tananyagtartalom és feladatprofilok alapján egy szakmailag és pedagógiailag lektorált feladatbankot létrehozni, és abból összeállítani az írásbeli mérőeszközt vizsgánként. Meg kell határozni a feladat megoldásra adható időtartamot és az elégséges eredmény százalékát (általában 51 %). A gyakorlati vizsga feladatai, szituációit szintén élethű körülmények közt kell megszervezni, azonban a gyakorlati vizsgán nem célszerű százalékos értékelést meghatározni, eben az esetben az egységes értékelési szempontok meghatározása alapján a megfelelt – nem felelt meg értékelés a helytálló.

A vizsga sikeres abszolválásával nem tekinthető az oktatás és a képességek megszerzésének folyamata befejezettnek. A képzési programban meg kell határozni az elsajátított képességek szinten tartási módját, gyakoriságát, az esetleges ellátásbeli szemléletek, új módszerek megjelenésének, változásának eljuttatását a képzettekhez. Az elsajátított ismeretek szinten tartásához a félévente végzett ismétlő gyakorlat szükséges, és legalább 5 évente egy új kurzuson való részvétel.

ÖSSZEFOGLALÁS

Összefoglalva elmondható, hogy akár békeidőben, akár a minősített helyzetekben kialakult sérülések, hirtelen egészségkárosodások legnagyobb ellensége az idő. Az az idő, amíg a szaksegítség a helyszínre érkezik az a társunknak, barátunknak, családtagunknak az életét jelentheti. Az idejekorán elkezdett és szakszerűen végzett elsősegélynyújtással életet menthetünk, maradandó károsodásoktól menthetjük meg a beteget. Ezért fontos, hogy minden időszakban minél többen legyünk képesek szakszerű és sikeres elsősegélyt nyújtani! Ehhez fontos azon szemlélet hirdetése, hogy az elsősegélynyújtás, harctéri elsősegélynyújtás készségszintű elsajátítása ugyanolyan fontos, mint a harcászat és lőgyakorlatok képességeinek elsajátítása.

Felhasznált irodalom

[1] Pápai Tibor: Elsősegélynyújtás, Műszaki Kiadó, Budapest 2010

[2] http://net.jogtar.hu/ 2011. november 13.

[3] E. John Wipfler et all: Tactical Medicine Essentials Jones and Bartlett Publishers 2011. Canada

[4] Jones and Bartlett: Combat Medic Field Reference, 2005, 13-23, 209-214.

[5] 1/2011. (I. 7.) NEFMI rendelet: Az egészségügyért felelős miniszter hatáskörébe tartozó szakképesítések szakmai és vizsgakövetelményeinek kiadásáról. Magyar Közlöny 2011. 1. szám

[6] Elsevier Mosby: Basic and Advanced Prehospital Trauma Life Support, Military edition, 2005

[7] A Magyar Resuscitatios Társaság állásfoglalása az újraélesztés oktatásáról, http://www.reanimatio.com/ 2011. november 13.

[8] Mark. W. Wieting et all: 68w Advanced Field Craft: Combat Medic Skills, Jones and Bartlett Publishers 2010. Canada

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Tóth György – Huszár András – Kormos Tímea
toth.gyorgy@mentok.hu – andras.huszar@aok.pte.hu – poisonperzon@gmail.com

A HALOTTKÉMI RENDSZERRŐL ÁLTALÁBAN

Absztrakt

A halottvizsgálat, a halottakkal kapcsolatos intézkedések, a halál körülményeinek megállapítása, vizsgálatai az egyes országokban eltérő szabályozás alatt állnak. Magyarországon a korábbi halottkémi rendszert felváltotta a kizárólag orvosi, mentőtiszti tevékenység, míg az Amerikai Egyesült Államokban, az Egyesült Királyságban a mai napig is jellemzően halottkémi rendszerben történik a halálmegállapítás, a halálhoz kapcsolódó vizsgálatok elvégzése.
A halottkémi rendszer jellegzetességét adja az alapvetően nem orvosi végzettségű személyek tevékenysége, melyhez kapcsolódhat a szakértők - törvényszéki patológusok - vizsgálata a halál körülményeinek felderítésében.

The death investigation, the statement of the circumstances of related measures, the death, his examinations look under the regulation differing in the single countries with the dead persons.
The earlier coroner system was replaced by him in Hungary the exclusively medical, ambulanceman activity, while the death statement happens in a coroner system characteristically until the today's day in United States of America, United Kingdom, the accomplishment of the examinations being attached to the death.
It gives the characteristic of the coroner system fundamentally not the activity of persons with a medical qualification, which one may be attached to the experts - forensic pathologists - his examination in the exploration of the circumstances of the death.

Kulcsszavak: *halottvizsgálat, halottkém, halottkémi rendszer ~ death investigation, coroner, coroner system*

BEVEZETÉS

Az Amerikai Egyesült Államokban, az Egyesült Királyságban a halottkémi rendszer, a halottkémek munkája a helyszíni halálmegállapítás, a halál okának felderítése a halottvizsgálati tevékenység részét képezi. A XIX - XX. században Magyarországon is működő halottkémek feladatait később orvosi kompetenciává módosították, ennek megfelelően napjainkban a hazai gyakorlat szerint a halott vizsgálata, dokumentációja, a szükséges további intézkedések az elsőként észlelő orvos feladata.

A HALOTTKÉMI TEVÉKENYSÉG MAGYARORSZÁGON

Magyarországon az 1826-os „Utasítás a Magyar Országi Szabad Királyi Városokba elrendelt Halottkémek számokra" szabályozza először a halottkémlést, melynek célja, hogy a „város bátorságba tétessék, ne talán valaki tetszhalálban lévén, vagy holtnak képét viselvén, iszonyuképp elevenen temessék el." A halottkém feladata ezenkívül az erőszakos halál felderítése, a halálokok feljegyzése, a járványok jelzése volt. [1]

A valóban hatékony, korszerű egészségügyi szabályozás az 1876. évi XIV. törvénycikk,

valamint az 1876. VI. 4./ 31.025. számú belügyminiszteri rendelet volt, mely a temetés körüli, valamint ezzel kapcsolatos népegészségügyi teendőket is tartalmazta. [2]

A jogszabály alkotására szükség volt, hiszen az ország területén nem állt rendelkezésre elegendő számú szakember, aki ezt a közfeladatot elvégezte volna. Az elsődleges cél a halottak körüli eljárás egységes bevezetése volt, a kompromisszumos megoldást nem lehetett elkerülni, így a halottkémlést nem kizárólag az orvosok illetékességébe utalták.

Alapelvként szolgált, hogy a halottvizsgálatot csak hivatalos személyek végezhessék, továbbá ezen személyek kellő számban történő kirendeléséről minden községnek gondoskodnia kellett. Halottkém az ország területén tevékenységi jogosultsággal bíró „orvostudor vagy sebész" lehetett, valamint a szolgálat egyenletes hozzáférhetőségét biztosító, halottkémi vizsgával rendelkező kioktatott személy is teljesített feladatokat.

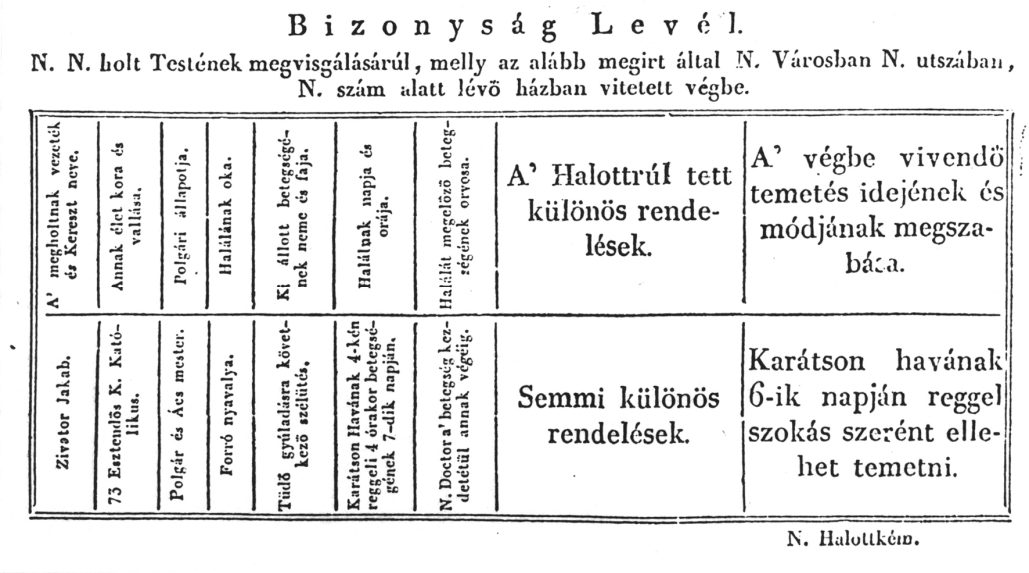
Az orvosi és sebészmesteri képesítéssel rendelkezők és a nem orvos halottkémek részére egyaránt pontos utasítás állt rendelkezésre, amely tételesen összefoglalta a haláleset kapcsán kötelező teendőket. A vizsgálatot a bejelentést követően haladéktalanul meg kellett kezdeni, klinikai halál (akkoriban „tetszhalál"-nak nevezték) gyanúja esetén az orvos, vagy sebészmester köteles volt elkezdeni az életműködések helyreállításának kísérletét, míg a nem orvos halottkém ilyen körülmény észlelésekor azonnal az orvost hívatta, majd ezt követően tehetett próbálkozásokat az újraélesztésre. A halott újraélesztésére, az életműködések vizsgálatára vonatkozóan Flór Ferenc tanításai még napjainkban is érvényes szabályokat tartalmaznak a helyszíni, sürgősségi ellátás során. [2]

Sikertelen újraélesztést követően a teendő a rendkívüli körülmények keresése, illetve kizárása volt.

A törvény, illetve a belügyminiszteri rendelet előírja, hogy a hatóságilag kirendelt halottkém igazolása előtt senkit sem szabad eltemetni. A halottkémek halottvizsgálati bizonyítványt állítanak ki (1. sz. ábra), amelyben feltüntetik a halál okát, bekövetkeztének idejét, az eltemetés ideje a halál beálltát követő 48 óra, amelyet a nyári melegben 36 órára lehetett csökkenteni, tetszhalál gyanúja esetén viszont 60 órára is ki lehetett tolni. [3]

A jogszabályok bevezetését követően Magyarországon kiépült a halottkémlés intézményes hálózata, minden község köteles volt megfelelő számú halottkémről gondoskodni. A jó erkölcsű jelentkezőket a körzeti orvos képezte ki, 1929-ben is csak a halottkémek 30 %-ának

volt orvosi végzettsége, a képesített és képesítés nélküli halottkémek számára kézikönyveket adtak ki.



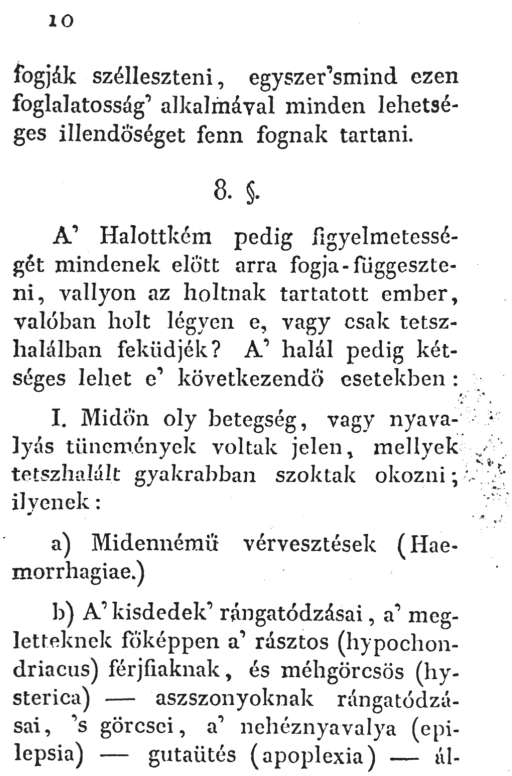
Bizonyság Levél.

N. N. holt Testének megvisgálásárúl, melly az alább megirt által N. Városban N. utszában, N. szám alatt lévö házban vitetett végbe.

A' megholtnak vezeték és Keresztt neve.	Annak élet kora és vallása.	Polgári állapotja.	Halálának oka.	Ki állott betegségének neme és faja.	Halálnak napja és órája.	Halálát megelőző betegségének orvosa.	A' Halottrúl tett különös rendelések.	A' végbe vivendö temetés idejének és módjának megszabáca.
Zivatar Jakab.	73 Esztendös K. Katólikus.	Polgár és Ács mester.	Forró nyavalya.	Tüdö gyúladásra következö szélütés,	Karátson Havának 4-kén reggeli 4 órakor betegségének 7-dik napján.	N. Doctor a' betegség kezdetétül annak végéig.	Semmi különös rendelések.	Karátson havának 6-ik napján reggel szokás szerént elhet temetni.

N. Halottkém.

1. ábra. Halottvizsgálati bizonyítvány a XIX. századból
Forrás: Lakner Judit: A halál megállapítása. A tetszhalott. História, 056 (1991)
http://www.tankonyvtar.hu/site/img/historia/1991_91-056_23_Lakner3_original.jpg
letöltve: 2010. 11. 15.



10

fogják széllleszteni, egyszer'smind ezen foglalatosság' alkalmával minden lehetséges illendöséget fenn fognak tartani.

8. §.

A' Halottkém pedig figyelmetességét mindenek elött arra fogja-függeszteni, vallyon az holtnak tartatott ember, valóban holt légyen e, vagy csak tetszhalálban feküdjék? A' halál pedig kétséges lehet e' következendö esetekben:

I. Midön oly betegség, vagy nyavalyás tünemények voltak jelen, mellyek tetszhalált gyakrabban szoktak okozni; ilyenek:

a) Midennémü vérvesztések (Haemorrhagiae.)

b) A' kisdedek' rángatódzásai, a' megletteknek föképpen a' rásztos (hypochondriacus) férjfiaknak, és méhgörcsös (hysterica) — aszszonyoknak rángatódzásai, 's görcsei, a' nehéznyavalya (epilepsia) — gutaütés (apoplexia) — ál-

2. ábra. Részlet az 1876. VI. 4./ 31.025. számú belügyminiszteri rendeletből a halottkém teendőire vonatkozóan
Forrás: Lakner Judit: A halál megállapítása. A tetszhalott. História, 056 (1991)
http://www.tankonyvtar.hu/site/img/historia/1991_91-056_23_Lakner5_or
letöltve: 2009. 11. 15.

A halottkémléssel kapcsolatban felmerülő kérdések között szerepelt, hogy a rendkívülikörülmények kapcsán mennyiben merül ki a halottvizsgálatot végző felelőssége, mire terjed ki a kompetenciája és mely ponton ér véget feladata.

Rendkívüli halálesetnek minősült, ha: „A hulla megvizsgálásakor erőszakos halál gyanúja, vagy jelei állapíthatók meg (öngyilkosság, gyilkosság), ha az egyén rögtöni halállal múlt ki, a talált hullák, ha a halál olyan betegség következtében állott be, amely ragályos járvánnyá szokott kifejlődni, a halva született magzatok, tekintet nélkül korukra és kifejlődésükre, valamint a gyógykezelés nélkül elhalt 7 éven aluli gyermekek halálesetei" (2. sz. ábra).

Ha erőszakos halál gyanúja merült fel, a rendkívüli körülményt azonnal jelenteni kellett,mivel az rendőrhatósági intézkedést vont maga után, s a korabeli utasítás szerint a halottkém mindent meg kellett, hogy tegyen a nyomozás segítése érdekében, például lefoglalta a helyszínen a gyanús tárgyakat, vagy mérgeket. Amennyiben azonban a rendőrhatósági eljárás során bizonyosságot nyert az idegenkezűség, véget ért a halottkém illetékessége, hiszen ebben az esetben a bűnvádi perrendtartásról szóló 1896. évi XXXIII. törvénycikk értelmében szakértőket (két orvost) kellett kirendelni halottszemle és boncolás céljából.

A halottvizsgálatot végzőnek napjainkban is felelőssége van abban, hogy keresse azesetleges idegenkezűség nyomait.

A halottvizsgálat jellegzetességei napjainkban

Ha párhuzamot próbálunk vonni a napjainkban jellemző helyzettel, a gondok elsősorban a területi ellátás során bekövetkező halálesetek kapcsán adódnak. A mai rendszer alapjai az 1972. évi II. törvény hatályba lépésével kezdődött, mely orvosi kompetenciaként tartalmazza a halálesetek vizsgálatát. A rendkívüli halálesetek felismerése az ügyeleti ellátási időben bekövetkező halálozások során is jelentkezhetnek. Ilyen esetekben a halottvizsgálatot végző orvos sokszor nem rendelkezik kellő információval, a hozzátartozók nem tudják átadni a korábbi orvosi iratokat, zárójelentéseket, nem tudják elmondani a kórelőzményt.

Mindezek hiányában az orvosok gyakran általános halálokokat jelölnek meg, amelyek csekély információtartalma csak a későbbi adatfeldolgozás során válik nyilvánvalóvá. [2]

A mentőtiszt szerepe a halál megállapítása során

A jelenlegi szabályozás a mentőtiszt feladatai között is szerepelteti a halál megállapítását, a rendkívüli halálesetek felismerését. [2]

A mentőtiszt egészségügyi főiskolán diplomát szerzett, sürgősségi ellátásban szakértelemmel rendelkező személy, akinek kompetenciakörébe tartozik a halál megállapítása, az újraélesztés, a halál feltételezett okának megjelölése, rendkívüli halál esetén a szükséges intézkedések kezdeményezése.

Igazgatási értelemben nem jogosult halottvizsgálati bizonyítvány kiállítására, tehát halottvizsgálatot nem, csak halál megállapítást végez, melyről dokumentációt készít, ebben tájékoztatást nyújt a halál tényéről, időpontjáról, az esetleges beavatkozásokról, rendkívüli eseményekről, a további intézkedés a háziorvos, ügyeletes orvos, illetve a rendőrség feladata.

A közterületi haláleset mindig rendkívülinek számít, itt a karhatalom (rendőrség) veszi át a folyamat irányítását.

HALOTTKÉMI RENDSZER AZ EGYESÜLT KIRÁLYSÁGBAN

Az Egyesült Államokban, illetve az Egyesült Királyságban a XIX. századtól kezdődően figyelhető meg a halottak vizsgálata során a halottkémek jelenléte.

Ahogyan Magyarországon is, szükség volt arra, hogy a halottvizsgálatot szakember végezze megfelelő jogszabályi háttér mellett, az erre vonatkozó, ma is érvényes szabályozás az 1988. évi Halottkémi Törvény, azóta számos jogszabályi reformjavaslat is kidolgozásra került. [4] [5]

A jogszabály részletesen meghatározza a halottkém feladatait, az egyes eljárásokra vonatkozó szabályokat, a halottkém kinevezését, felmentését, díjazását, nyugdíjazását. Ennek értelmében a főváros, London kerületeiben, illetve minden nagyvárosban szükséges az egyes közigazgatási körzetekben halottkémek kinevezése, mely pályázat útján történik, s erről az illetékes Tanács dönt, egyidőben a szakállamtitkár tájékoztatása mellett.

A halottkémi feladatok ellátásához szakképesítés szükséges, mindemellett a halottkém lehet ügyvéd, vagy jogi ismeretekkel rendelkező orvos is, amennyiben 5 évnél hosszabb időtartamú gyakorlatra tett szert.

A jogszabály megfogalmazza a halottkém illetékességét, a helyettesítését, konkrét feladatait:

- Általános halottkémi szemle tartása az alábbi esetekben kötelező a körzeten belüli halálesetekkel kapcsolatban:
  - ha erőszakos, vagy nem természetes halál következett be;
  - ha a hirtelen halál ismeretlen okkal történt;
  - ha börtönben, vagy olyan helyen következett be a halál, ahol egyéb jogszabályok kötelezik a szemle megtartását.

Saját hatáskörben dönt arról, hogy a bekövetkezett halál igazságszolgáltatási eljárás aláesik-e vagy sem, s ennek megfelelően vizsgálja, illetve jelentést tesz az illetékes szervek felé.Vizsgálatot folytat a halál okának és körülményeinek tisztázása érdekében, független szakértőket (nyomozót) vonhat be a vizsgálatba, tanúkat hallgathat meg, hozzátartozókat kérdezhet ki, kezdeményezhet további, szakértelmét meghaladó vizsgálatokat.

A halottkém tevékenysége:

- pathológiai vizsgálatok, boncolások kezdeményezése, az áldozatok azonosítása, traumák, jellegzetes sérülések, a halál időpontjára utaló jelek keresése;
- az elhunyt személy azonosítása, a halál okának, módjának és körülményeinek megállapítása;
- boncoláson, méregtani elemzésen történő részvétel, annak dokumentálása;
- halotti bizonyítvány kitöltése, megnevezve a halál kiváltó okát;
- megfigyeli és rögzíti a test elhelyezkedését, jellegzetességeit, a kapcsolódó bizonyítékokat;
- a beteg kórelőzményét, betegségeit dokumentálja;
- tárgyak, a beteg használati eszközeinek vizsgálata, mint pl.: gyógyszeres üvegek, öngyilkossági feljegyzések;
- teljes jelentés és dokumentáció a halott vizsgálatával kapcsolatban;
- az elhunytak elszállításának kezdeményezése és ellenőrzése;
- a helyszínen tartózkodók kikérdezése, információgyűjtés a halál okának megállapítására vonatkozóan;
- biológiai- és vegyi terrorizmus felismerése;
- a fertőző betegségek felismerése;
- az egészségügyi ellátás minőségének ellenőrzése. [5]

HALOTTKÉMI RENDSZER AZ AMERIKAI EGYESÜLT ÁLLAMOKBAN

A halottkémi rendszer angol mintára, a XVII. századtól kezdődően kezdi működését, kezdetben a rendőri feladatokkal összhangban, elsőként 1860-ban, Maryland-ben jogszabály fogalmazza meg a halottkém feladatait. [6]

A modern Amerikában évente 2 millió haláleset 20 %-ában történik halottvizsgálat orvos, vagy halottkém által.

2002-ben felmérés történt az egyes államok tekintetében a halottvizsgálattal kapcsolatban, az elemzés eredményeképpen 22 államban orvosszakértői rendszer, 11 államban halottkémi rendszer, 18 államban vegyes (orvosi-halottkémi) rendszer működik. [7]

Halottkémi vizsgálati rendszer

Az államokban és egyes megyékben a halottvizsgálatot végző személy a halottkém, aki 18 évnél idősebb, amerikai állampolgár, az adott megye állandó lakosa, rendszerint 4 éves szolgálati ciklusra választott személy.

A halottkém felelős a vizsgálatok kezdeményezésére és lefolytatására a halál okára és módjára vonatkozóan azokban az esetekben, melyek a hatáskörébe tartoznak, beleértve:

- az erőszakos, hirtelen, vagy váratlan, illetve a gyanús halálozásokat;
- a drogok és mérgek által okozott halálozásokat;
- az orvosi ellátás közben történt haleseteket;
- a munkavégzés közben bekövetkezett haláleseteket;
- a karhatalmi intézkedés közben történt haláleseteket;
- terhességben történt haláleseteket;
- gyógyintézetben, pszichiátrai intézetben, kórházi szállítás során történt haláleseteket;
- idősek, szociális otthonokban bekövetkezett haláleseteket;
- azokat az eseteket, amikor nincs jelen orvos a halál bekövetkezése alatt.

A halottkém szakértőt vehet igénybe (törvényszéki kórboncnok) a halott vizsgálatához.

Az orvosszakértői rendszerben a halottvizsgálatot az első észleléstől kezdődően orvos(pathológus) végzi, aki speciális ismeretekkel és képesítéssel rendelkezik.

Az orvosszakértő és halottkém feladatai között olyan tevékenységek is szerepelnek, amelyek nemcsak a büntetőjogi rendszer számára fontosak, hanem a közegészségügy, a közbiztonság, az egészségügyi ellátás, az oktatás és kutatás területén is hasznosak. [8]

A halottvizsgálati rendszer

A halott vizsgálatához elengedhetetlen a szükséges speciális egészségügyi ismeretek megléte. A helyszínen a holttest vizsgálata és a bizonyítékok összegyűjtése történik, kiegészítve a fizikális és laboratóriumi vizsgálattal, a diagnózis és a korábbi betegségek felvételével.

A legfontosabb cél az objektív bizonyítékok feltárása a halál okára, idejére és módjára vonatkozóan, melynek továbbítása történik az igazságszolgáltató rendszer felé.

Randy Hanzlick közleményében hangsúlyozza a halottvizsgálat jelentőségét és társadalmi fontosságát a büntető igazságszolgáltatás és a közegészségügy területén, mely bizonyítékot szolgáltat a vétkes bűnösségére és az ártatlan védelmére, függetlenül attól, hogy a vád gyilkosság, gyermekbántalmazás, gondatlanság, vagy más bűncselekmény.

A halottvizsgálatok támogatják a polgári peres ügyeket, mint például a műhiba pereket, személyi sérüléseket, vagy életbiztosítási követeléseket. A vizsgálatok több szempontból is döntő fontosságúak a közegészségügyi gyakorlat és kutatás számára, beleértve az epidemiológiai megfigyelést, a megelőzést, mely nemcsak a sérülések megelőzését és ellenőrzését, hanem az öngyilkosság, az erőszak, illetve a gyógyszerekkel való visszaélést is vizsgálja.

A halottvizsgálatot halottkémek, vagy orvosi vizsgálóbiztosok végzik, akik orvosok, patológusok, igazságügyi patológusok lehetnek, ők biztosítják az orvosi szakértelmet, értékelik a kórtörténetet és végzik az elhunyt fizikális vizsgálatát. A halottkém egy megválasztott, vagy kinevezett tisztviselő, aki általában egy megye területén rendelkezik jogosultsággal és gyakran nem rendelkezik orvosi végzettséggel. [8]

ÖSSZEFOGLALÁS

A halálmegállapítás, a halottak vizsgálata az Amerikai Egyesült Államokban, az Egyesült Királyságban - Magyarországtól eltérően - halottkémi rendszerben történik, melyben orvosok, ügyvédek, valamint nem orvos képzettségű személyek is helyet kapnak.

A jogi szabályozás meghatározza az egyes feladatköröket, kompetenciákat, jogokat és kötelezettségeket, melyek a helyszíni, valamint a későbbi vizsgálati tevékenység alapját képezik.

Hong Kong-ban a halottkémi rendszer változása és fejlődése várható a jövőben, melyhez az orvosi tevékenység előtérbe kerülése, a karhatalmi szervek felügyeletének és beavatkozásának mérséklése, az ügyvédi-jogi képviselet csökkenése szükséges. [9]

Magyarországon a halottkémi rendszert felváltotta az orvosi kompetenciakörbe tartozó halottvizsgálat, azonban a jogi szabályozás a halál megállapítására, a halottal kapcsolatos helyszíni tevékenységre sürgősségi ellátásban jártas, nem orvos végzettségű szakembert is feljogosított.

Felhasznált irodalom

[1] Lakner Judit: A halál megállapítása. A tetszhalott. História, 1991 http://www.tankonyvtar.hu/historia-1991-056/historia-1991-056-halal, letöltve: 2011. 10.01.

[2] Kádár László, Prof. Balázs Péter: Temetés és haláleset kapcsán követendő eljárások dilemmái a modern közegészségügyi igazgatásban. Egészségtudomány, LIII. évf. 3 (2009) 8-19. http://www.higienikus.hu/egeszsegtudomany/cikk/2009_3.pdf, letöltve: 2011. 10.01.

[3] Hanák Péter: A halál Budapesten és Bécsben. In: Hanák Péter: A Kert és a Műhely. Gondolat, Budapest, 1988

[4] Office of Public Sector Information: Coroner's Act 1988. 1988 Chapter 13. Arrangement of sections. http://www.opsi.gov.uk/acts/acts1988/ukpga_19880013_en_1#Legislation-Preamble, letöltve: 2011. 09. 30.

[5] Tom Luce: Coroners and death certification law reform: the Coroners and Justice Act 2009 and its aftermath. Medicine, Science and the Law, Volume 50 (2010 october) 171-178.

[6] Patricia W. Iyer,Barbara J. Levin,Mary Ann Shea: Medical legal aspects of medical records. Lawyers & Judges Publishing Company Inc; 2006 http://books.google.hu/books?id=t5_EWfjODYC&pg=PT870&lpg=PT870&dq=coroner+system&source=bl&ots=bbkqSDDFr_&sig=Khq0nlHajBfp8Hoi_ggLllsxk&hl=hu&ei=olXvSq28C5H6_AbqrCZDw&sa=X&oi=book_result&ct=result&resnum=2&ved=0CA4Q6AEwATgo#v=onepage&q=coroner%20system&f=false, letöltve: 2011. 09. 30.

[7] Randy Hanzlick, Debra Combs: Medical Examiner and Coroner Systems: Hystory and trends. The Journal Of the American Medical Association, March 18, 279 (1998) 870-874.

[8] Randy Hanzlick: Options for Modernizing the Ontario Coroner System. The Inquiry into Pediatric Forensic Pathology in Ontario, 2008 http://www.attorneygeneral.jus.gov.on.ca/inquiries/goudge/policy_research/pdf/Hanzlick_Options-for-Modernizing.pdf, letöltve: 2011. 09. 30.

[9] B. Knight: The future of the coroner's system in Hong Kong. Hong Kong Medical Journal, Jun 2, 2 (1996) 217-218. http://www.docstoc.com/docs/2458895/The-future-of-the-coroners-system-in-Hong-Kong
letöltve: 2011. 09. 30.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Csépainé Széll Pálma
palma.szell@gmail.com

HELYI KÖZIGAZGATÁSI REFORM MAGYARORSZÁGON

Absztrakt

Két évtizednek kellet eltelnie ahhoz, hogy a közigazgatási gyakorlat makacs tényei alapján szembesülni lehessen a korábbi közjogi elképzelések hiányosságaival. A közigazgatási-korszerűsítési kormányprogramnak adott kormányzati ciklust átívelő javaslata az önállóság és a központosítás viszonyát próbálja helyes mederbe terelni, elsősorban a helyi önfinanszírozó képesség „újjászervezésével". Ez természetszerűen azt kívánja meg a helyi közösségektől, hogy szakítsanak az eddigi gazdaságszervező, intézményfenntartói és szociálpolitikai beidegződésekkel. Az is megállapítható, hogy a központi és a helyi hatalom viszonyában nem sikerült kialakítani azt az ideálisnak mondható munkamegosztási kombinációt, amely a két hatalmi szféra érdekegyeztetési mechanizmusának működtetését is egyensúlyban tartja. Ez a „kettős ráutaltság" a helyi önkormányzatok fejlesztése szempontjából nem jelent mást, mint a helyi és a központi hatalmi szféra együttes korszerűsítésének sürgető szükségszerűségét.

Two decades had to pass to face the facts of administrative practice's deficiency. The government's program dealing with administrative-development was focusing on the improvement of autonomy in relation with centralization, mainly through self-financing, This demanded that the local communities break away from economic organization, maintaining institutions and social policy habits It is also concluded that in relation with the central and the local authority it was impossible to establish an ideal division of labor, that keeps them in balance with their interests. This double-dependence of local governments' development does not mean anything else, than the urgent need of development of the local authority in conjunction with the central authority.

***Kulcsszavak**: települési önkormányzat, helyi közszolgáltatás, alkotmány, önkormányzati modell ~ local government, local public service, constitution, local government model*

BEVEZETÉS

Reform, újraszervezés, racionalizálás, hatalomkoncentráció vagy szerves fejlődés? A téma megfogalmazása provokatívnak tűnhet, hiszen azt a benyomást keltheti, mintha ma lehetőség adódna egy szakmailag és társadalmi tapasztalatok alapján megerősített perspektívának a felvázolására. Vagy bizonyos körülmények – mindenekelőtt az alkotmányos berendezkedés átalakítása, az alaptörvény megalkotásának napi politikai kérdéssé válása, – kényszerhelyzetet teremtenek? Amennyiben elfogadjuk ez utóbbi megközelítést, érdemes a magyar önkormányzatiság jövőképéről néhány gondolatot megfogalmazni, függetlenül attól, hogy a közelmúlt tapasztalatait az elvárható szakmai és tudományos igényességgel nem, vagy csak kevés „szakmai műhelyben" vizsgálták.

Kiindulópontom az lehet – nem vitatva, hogy más megközelítés is figyelemre méltó –, hogy melyek a leggyakrabban megfogalmazott kritikai értékítéletek és az ezekre épülő javaslatok a különböző publikációkban, továbbá milyen igények fogalmazódnak meg az európai uniós tagsággal összefüggésben (a múltban és jelenben).[1] Nem hagyható figyelmen kívül azok a megközelítően sem koherens és egyben ellentmondásos közpolitikai tárgykörű megnyilvánulások sem, amelyek az utóbbi időben akár a napi sajtóban is megjelentek, vagy vitafórumokon elhangzottak.

A HELYI ÖNKORMÁNYZATOK A RENDSZERVÁLTOZÁS UTÁN

A magyar helyi önkormányzatok szerves fejlődését több tényező alapvetően és kedvezőtlenül befolyásolta. A 19. század harmadik harmadában kialakuló (polgári) helyi önkormányzatok bár számos vonatkozásban magukon viselték az előző feudális önkormányzati hatásokat, de megteremtették az európai önkormányzatisághoz való közeledés lehetőségét.

A rendszerváltozás után megalkotott önkormányzati törvény[2] különleges körülmények között született, amelyeket utólag már nehéz érzékeltetni, de néhányra érdemes utalni, hogy a két évtizedes működési tapasztalatok (problematikák) érthetőbbi váljanak. Mint közismert, a társadalmi-politikai következményei (nevezetesen a rendszerváltozás), az önkormányzatiságot nem a szocialista állam keretei között teljesítette ki, hanem a helyi önkormányzatokról szóló 1990. évi LVX. tv. (továbbiakban: Ötv.) alapján, az 1949.évi XX. tv. IX. fejezetében (továbbiakban: Alkotmány) foglalt alapnormáknak megfelelően.

Az elmúlt két évtized önkormányzati tapasztalatainak sokrétű elemzése szükségszerűség, de nem az elméletek számának gyarapítása okán, hanem a racionalitás, a hatékonyság és a társadalmi demokratizmus fejlesztése, valamint a közigazgatás modernizációja érdekében, különös tekintettel az európai uniós elvárásokra, illetőleg az ország által vállalt közös normákra, elvekre.

A jelzett időszakban visszatérő állami- társadalmi és közpolitikai célrendszer volt, hogy a helyi önkormányzatok mielőbb és lényegi tartalommal térjenek vissza az európai önkormányzatiság keretei közé. Megfogalmazódott ez a törekvés 1990 előtt is, amennyiben a szakmai-tudományos tapasztalatok alapján a kormányzat törvénybe foglalta a helyi tanácsok önkormányzati jellegét (1971), ennek kiterjesztését szorgalmazó kutatások több éven át folytak (1985-1990) és „a Helyi Önkormányzatok Európai Chartája" cím alatt az Európa Tanács által elfogadott egyezményhez (Európai Egyezmények 122. sz.) a csatlakozási szándékot a Minisztertanács elnöke az Európai Tanács parlamenti közgyűlésén bejelentette

[1] pl.: Rotterdami Program a kormányzásról és az európai integrációról,1997.május 29-30
[2] 1990. évi LXV. tv.

(1990. január 29-én). Ezt a folyamatot zárta le az Ötv. megalkotása, erre utal a törvény preambuluma is, megerősítve, hogy követi hazánk haladó önkormányzati hagyományait, továbbá az Európai Önkormányzati Charta alapkövetelményeit (továbbiakban: Karta).

Kiemelésre méltó, hogy hangsúlyt kap az Ötv. preambulumában is:

- a helyi közösségek önkormányzáshoz való joga, annak elismerése és védelme;
- a közügyek önálló és demokratikus ügyintézésének elve;
- a közösségek önszervező önállósága, az önkormányzáshoz szükséges feltételek biztosítása (értelemszerűen az állam részéről), a közhatalom demokratikus decentralizációjának elmozdítása.

Az Európai Unió (továbbiakban: EU) által is elfogadott fenti elvek jelennek meg az uniós normatívákban, elvekben. Ennek egyik meghatározó és részletes tartalmi elemekkel bíró okmánya az ún. rotterdami-program (továbbiakban: Program).[3] A Program – bár a kormányzást emeli ki címében – részletesen foglalkozik a demokrácia, a társadalom és a kormányzati hatalom kapcsolatával, az állami irányítás minőségével. Kiemeli, hogy: „a helyi demokrácia a demokratikus állam egyik alappillére. A választott helyi önkormányzatok bizonyos fokú ellenőrzést tesznek lehetővé a központi kormányzat gépezetének potenciális túlsúlya fölött. Amikor helyi önkormányzatról beszélünk, a közigazgatás kormányzásban betöltött szerepére is gondolunk. Ez azt is jelenti, hogy pontosan meg kell fogalmazni a szerepeket és a kapcsolatokat, illetve meg kell tanulni konstruktív módon kezelni a feszültségeket (amelyek egy közös térben működő két különböző szintű kormányzás között elkerülhetetlenek.) Az EU keretei között az együttes kormányzás vagy társkormányzás azt is jelenti, hogy rendezni kell a közigazgatás szervezeti egységei és az EU intézmények közötti kapcsolatot. Fontos, hogy az önkormányzatok igazgatási tevékenysége infrastruktúrát biztosít az integráció és a kohézió érvényesítéséhez. Ezen kívül a helyi önkormányzatok kulcsfontosságú szerepet játszanak a helyi polgári társadalom ösztönzésében és összefogásában, valamint a megfelelő együttműködés kialakításában. A közigazgatás felgyorsíthatja azoknak a körülményeknek a kialakítását, amelyek kedveznek a polgári társadalom fejlődésének.

Kétségtelen, hogy az elmúlt időszak tapasztalatai azt erősítik, hogy az említett elvek érvényesítése terén nem csak „tanulni” kell a kormányzatnak, hanem határozottabban kell törekednie azok törvényi megfogalmazására és gyakorlattá tételére, amelyhez egy új, tartalmában és szerkezetében megreformált törvényen vezet az út. A Program részletesen is kifejti a fenti gondolatokat, nevezetesen:

- a központi állam hatalmának ellensúlyozása, egyben a hatalom gyakorlásában való részvétel tanulása;
- a kölcsönös függés a közérdekre tekintettel;
- a hatalommegosztás és a pénzforrások megfelelő elosztása, a társkormányzás elve alapján;
- együttműködés a helyi polgári társadalom intézményeivel úgy, hogy közben ne tegyen kísérletet annak ellenőrzésére;
- a helyi stratégiai irányok kialakításában a partnerség és a konszenzus elve érvényesüljön;
- el kell ismerni a regionális eljárások sokszínűségét és ezek hozzájárulását a helyi önkormányzat elveinek érvényesüléséhez;
- a helyi önkormányzatok hozzájárulnak az EU politikai irányelvek megvalósításához és az országokon túli kapcsolatok kiépítéséhez (A Program 2. fejezet 3. pontja).

[3] „Rotterdami Program a kormányzásról és az európai integrációról”, záródokumentum, 1997. május 29-30-án, az Európai Unió holland elnökségének égisze alatt megszervezett konferencia.

A hatályos Ötv. indokolása megerősíti a fenti elveket és reményét fejezi ki, hogy az ilyen módon kiépült önkormányzati rendszer arra is képes lesz, hogy „korlátokat állítson a központosítás túlzó törekvéseivel szemben”.

Az önkormányzatok tapasztalatai e tekintetben erősen megoszlanak, nem kevés az olyan vélemény, amely szerint nem sikerült behatárolni a „túlzó törekvések” fogalmát, így a korlátok viszonylagossá váltak. A mindenkori kormányzatok nézetrendszere, pillanatnyi érdeke határozta meg, hogy mikor és mennyiben korlátozhatja a helyi önkormányzatok mozgásterét.

A magyar helyi önkormányzatokra vonatkozó alkotmányos alaptételek és törvényi szabályozás általános felülvizsgálatának szükségessége két megközelítésben is felmerül.

A helyi önkormányzatok működésük során mind gyakrabban érzik, hogy nem tudnak megfelelni a velük szemben támasztott követelményeknek. A feladat- és hatáskör tekintetében nincs összhang, illetve anyagi forrásaik nem adnak fedezetet a közösségi szükségletek kielégítésére (közismert példák: egészségügyi és oktatási-nevelési intézmények szolgáltatási színvonalának alakulása, az intézmények felszámolása vagy átszervezése, illetve állami szférába történő átadása). A belső működési ellentmondások nyilvánossá válása, különös tekintettel a testületek és tisztségviselők vonatkozásában, amit a politikai érdekviszonyok esetenként a végletekig feszítenek. Számos zavaró tényező alakult ki az önkormányzati igazgatás szervezeti rendszerében is (pl.: feladat- és felelősségi viszonyok tisztázatlansága,a testületi irányítás és a szervezet vezetésének napi konfliktusa stb.).

A közigazgatás egészéért felelős kormányzat, illetve a helyi önkormányzatok törvényességi ellenőrzése tekintetében szereppel bíró szervek (kormány és megfelelő szervei), ugyancsak gyakori kritikai észrevételekkel élnek a mai törvényi szabályozás és az észlelt gyakorlat számos területén. A központi akaratérvényesítés korlátjaként megjelenő önkormányzati önállóság, annak minden típusa: a mérlegelő, teljes önállóság, illetve a végrehajtási önállóság vonatkozásában, ezért a legegyszerűbb megoldásra törekednek: a helyi közfeladatok lehető legnagyobb részét szeretnék átvinni az állami közigazgatási szférába, s ez a folyamat az utóbbi években felgyorsult, esetenként az önkormányzatok tehermentesítése indokával.

A várható változások előjelei alapján nehezen megítélhető az általános tendencia; a reformok (vagy új alapokra helyezése a helyi önkormányzatok alkotmányos státuszának) tekintetében azonban néhány támpont kialakítható.

Megkerülhetetlennek látszik, hogy a helyi önkormányzatokról az alkotmány a Karta alapján alapelveket szabályozzon (a nemzetközi egyezmény erre kötelező normákat is tartalmaz), ha nem akarják a kötelezettségszegést felvállalni. Nem hagyható figyelmen kívül, hogy a Karta az alkotmányi szabályozás tekintetében is mozgásteret enged a kormányzatnak, mivel a helyi önkormányzás elvének elismerését az alábbiak szerint határozza meg: „…a belső jogalkotásban és amennyiben lehetséges alkotmányban is el kell ismerni…” (2. cikkely).

Más pontoknál „…az alkotmány vagy törvény…” determinációt találunk (pl.: 4.cikkely 1. pont; 8. cikkely 1. pont; 9. cikkely 2. pont, stb.). Így sok függ a döntéshozók értékítéletétől, illetőleg attól, hogy a helyi önkormányzatok (azok érdekszövetségei), milyen módon és milyen társadalmi támogatással tudnak megnyilvánulni.

Bonyolultabb kérdés, hogy az európai uniós alapelvekhez, elvárásokhoz való viszony mennyiben és milyen jogalkotási formákkal realizálódik. A Programban megfogalmazottak vagy közösségi elvárások egybeesnek a közösségi vívmányokat eredményesen megvalósítani képes közigazgatás (állam, önkormányzat) létrehozásának igényével, amely tartalmilag az alábbiakat jelenti:

a tagállami közigazgatás legyen megbízható;

- a közigazgatás működése legyen átlátható és
- létrejötte, működése demokratikus elveken alapuljon.[4]

Az európai tendenciák közös vonása, hogy a közigazgatás területi szintjén elhelyezkedő egységek (pl.: régió) szerepköre erősödik és számuk csökken. Ez a regionalizáció azt is lehetővé teszi, hogy a központi állami szervek feladat- és hatásköreit, valamint az anyagi erőforrásokat decentralizálják a régiókhoz (állami vagy önkormányzati területi egység egyaránt szóba jöhet).

Európai viszonylatban a helyi önkormányzatok tekintetében a következők emelhetők ki:

- a helyi önkormányzatok (és igazgatási szerveik) többszintűek, de nem egymás alá-fölé, hanem egymás mellé rendeltek, azonos jogállásúak, eltérő feladatokkal;
- tevékenységük (feladat- és hatáskörük, illetve felelősségük) a helyi közügyek széles körére terjed ki;
- feladataik nagy hányada a közösségi szolgáltatás köré csoportosul (pl.: a településüzemeltetés, a településfejlesztés, a humánszolgáltatások, térségi koordináció és fejlesztés stb.);
- az önkormányzati jogkörök letéteményese a lakosság által választott képviselők (együtt : önkormányzat), a helyi igazgatási szervezet a választott testület irányítása – és felelőssége – alatt működik;
- a helyi önkormányzatok széleskörű nemzetközi kapcsolatokat építenek ki, regionális politikájuk átlépheti a tagállami határokat.

Az állam (a központi hatalom) és a helyi önkormányzatok kapcsolatának történetisége korábban sem volt zavartalan, csak a formák és a problémakezelés elvei és gyakorlata változott. Az önkormányzati rendszer – a korai és a klasszikus egyaránt –, a központi bürokrácia (az állami hatalom) ellenében jött létre, a helyi érdek megfogalmazója és képviselőjeként, hangoztatván, hogy a községek (a települések) eredeti, az államot megelőző entitások, azaz önállóságuk nem az államtól ered, így azt az állam nem is vonhatja el. Ez a felfogás, a korai önkormányzatiságra jellemző függetlenségi eszme az évszázadok során szelídült, ma már az európai alkotmányok ettől távolabb kerültek, de a község autonómiája védelmében az alkotmánybírósághoz fordulhat. Mára az önkormányzatok az európai államokban „belesimultak" az egységes közhatalmi szervezetrendszerbe, illetve a közigazgatásba, annak alrendszereként, belső korlátozott önrendelkezési joggal működnek.

Az 1949.évi XX. törvény szerint az önkormányzáshoz való jog a helyi választópolgárok kollektív alapjoga.[5] Megkerülhetetlenné vált azonban az önkormányzáshoz való jog alanyának és tartalmának vizsgálata is. Erre a kérdéskörre adott választ az Alkotmánybíróság, amikor az alapjogokkal összefüggésben egy határozatban megállapította, hogy azok valójában olyan hatáskörcsoportok, amelyek az önkormányzatok – elsősorban a kormánnyal szembeni – önállósághoz elengedhetetlenek, és amelyek címzettje nem a helyi választópolgárok közössége, hanem a képviselő-testület.[6] Minden esély meg van arra, hogy ez a törvényi szabályozás továbbra is része legyen az alapjogi normáknak. Indokolt jelezni azt is, hogy Nyugat-Európa számos államában érzékelhetően felerősödött az a közgondolkodás és ennek eredményeként alkotmányjogi szabályozás, amely következtében a helyi önkormányzatok alkotmányos garanciáira vonatkozó rendelkezések száma gyarapodott.[7] A fentiekre is

[4] Jacques Forunier: A megbízható közigazgatás, Magyar Közigazgatás, 1997. 47. évf. 10. sz. pp. 631-640.
[5] Ezt a természetjogias felfogást nem kevés kritika éri.
[6] Szente Zoltán: A helyi területi önkormányzatok alkotmányos szabályozásának elvei, de lege ferenda – Magyar Közigazgatás, 1994. 44. évf. 6-7. sz. pp. 364- 387.
[7] Kaltenbach Jenő:Közigazgatás és/vagy önkormányzat; A magyar közigazgatás korszerűsítésének elvi és gyakorlati kérdései, szerk.: Fogarasi József, Unió Kiadó, Budapest, 1996.

tekintettel – az alkotmányos garanciák erősödését tapasztalva – a helyi önkormányzatok és az állam viszonyrendszerét vizsgálva olyan alkotmányos szabályozás látszik kialakíthatónak, amelyben a közigazgatás egységes ugyan, de a centralizáció és a decentralizáció egyensúlya érvényesül. Miután ez az egyensúly spontán módon mindig centrális irányban mozog, alaptörvényi szinten kell kiépíteni egy ennek gátat szabni képes törvényi keretet.

Ezt az alapelvrendszert részben az alaptörvényben, részben az önkormányzatokról szóló törvényben célszerű rögzíteni. Ezek köre gazdagabban vagy szűkebben is meghatározhatók, néhányra azonban érdemes utalni.

Az egyes szintek között nincs alá-, fölérendeltségi viszony, az állam központi szerve azonban a helyi és a területi önkormányzatok felett törvényességi ellenőrzést vagy felügyeleti jogot gyakorol. Ugyanakkor az önkormányzatot jogvédelem illeti meg mind felülről, mind az alulról jövő korlátozás tekintetében, ezt a védelmet a bíróság biztosítja. A feladatok és hatáskörök a központi, a középszintű és a helyi szervek – az állam és a helyi önkormányzatok tekintetében – megosztottak. A hatáskör-telepítés a szubszidiaritás alapelvére épül, azok a helyi közügyek, amelyek teljesen vagy túlnyomó részben helyi érdekeket érintenek és az adott körben megoldhatóak, helyi (települési) hatáskörbe tartoznak. Az előző elvre tekintettel, az egy település határain belül meg nem oldható feladatokat középszintre célszerű telepíteni, az ország minden polgárát érintő, egységes érdekrendszerbe tartozó közügyek a központi kormányzati döntési kompetenciába kerülnek. Az önkormányzati szintek közötti megállapodással (konkrét települési és területi önkormányzatról van szó) a közfeladatok átadhatóak vagy megoszthatóak. A települések (területek) határvonalainak, jogállásának megváltoztatása tekintetében az állam rendelkezési joga és a választópolgárok kollektív joga, döntési kompetenciája.

A „hogyan és hova tovább?” kérdés megfogalmazása gyakori a mai szakmai tudományos közéletben. A válaszok azonban egyre differenciáltabbak és ellentmondásosak, amit számos tényező befolyásol. Ezek közül kiemelkedő jelentőséggel bír a társadalmi-politikai értékválasztás (egyszerűbben: a pártpolitika), a szakmai vagy tudományos ismeretek mélysége, a helyi önkormányzatokhoz fűződő kapcsolat tartalma és annak egyes szintjei is befolyásoló tényezők; továbbá a szinte felsorolhatatlan objektív és szubjektív körülmények (pl.: a törvényi reformra szánt előkészítő munka feltételrendszere stb.).

Ezért vállalható, hogy ez alkalommal sem lehet teljes körűen megrajzolni a szükséges változások (esetleg reformirányok) tartalmát, illetve a törvényi módosítások vagy új törvényben a jelenlegitől eltérő szabályozás egyes elemeit, de a főbb csomópontokról szólni kell, nevezetesen:

- a helyi önkormányzás szintjei;
- az önkormányzati feladatok és hatáskörök meghatározása;
- a testületek kialakítása, létszáma, belső szervezeti-működési normái;
- a helyi önkormányzatok (és igazgatási szerveik), valamint a kormányzat kapcsolatai;
- a helyi önkormányzatok jogvédelme.

AZ ÖNKORMÁNYZATI SZINTEK

A települések, mint alapkategóriák viszonylag stabil egységei a rendszernek. A mintegy 3200 településen belül azonban jelentős nagyságrendi különbségek adódnak. Megfigyelhető a városok számának erőteljes emelkedése és vonáskörzetükre gyakorolt gazdasági-kulturális és közigazgatási hatásuk erősödése. Ebben a vonatkozásban egy önkormányzati reform nem valószínű, hogy más tendenciákat bontakoztathat ki.

Alapvető gondokkal küzdenek, az un. kisközségek, amelyek a helyi önkormányzás és igazgatás tekintetében a működő képtelenség határán élnek. Elég, ha csak azokra a

feladatokra gondolunk, amelyek nélkül bármely önálló település elképzelhetetlen: egészséges ivóvízellátás, alapfokú oktatás, egészségügyi és szociális alapellátás, közvilágítás, helyi közutak és köztemető, a nemzeti és etnika kisebbségekkel kapcsolatos feladatok.

Az önálló települési együttélés az előzőeken túlmenő közösségi szerepköröket is igényel:

- településfejlesztés, településrendezés;
- az épített és természeti környezet védelme;
- a lakásgazdálkodás, a vízrendezés és csapadékvíz elvezetése, a csatornázás;
- a településtisztaság biztosítása;
- közművelődési tevékenység, a helyi sportélet támogatása; az egészséges életmód közösségi feltételeinek az elősegítése;
- a szociális és egészségügyi alapellátás.

A középszintű feladatok ellátása ma már lényegében a városok (megyei jogú városok) és a megyék szintjén és felelősségi körében jelenik meg. Ez a helyzet a jövőben is megmarad – nincs más reális alternatíva – csak az kérdéses, hogy ebben milyen szerepe lesz a társulási szándéknak, illetve a törvényi szabályozásnak.[8]

A főváros területi-szerkezeti viszonyainak - kialakulása, több évtizedes tapasztalatok, kétszintű önkormányzat, régi és jelenkori reformkísérletek sorozatának - vizsgálata a maga összetettségére tekintettel önálló megközelítést igényelne. Annyi mindenesetre megállapítható, hogy az elmúlt hat évtizedben nem volt olyan többéves időszak, amikor a döntéshozók vagy/és főleg az érintettek elégedettek lettek volna a meglévő tanácsi, illetve önkormányzati törvényi szabályozással. Ez a problematikus helyzet napjainkban már akuttá vált, ezért az alapvető viszonyok rendezése nélkül nincs jó megoldás.

Már az első önkormányzati ciklus végén nyilvánvalóvá vált, hogy a fővárosra vonatkozó szabályozás egyike a leggyengébb Ötv. elemeknek, gond a feladat- és hatáskörök telepítése, az egységes fővárosi érdek megjelenítése. Ezért lehet egyetérteni Sóvágó László országgyűlési képviselőnek (MDF) azzal a megállapításával, hogy: „…A szabályozás újragondolása elkerülhetetlen…" A politika kiütéses győzelmet aratott, háttérbe szorultak a szakmai szempontok, ezzel a törvénnyel nagyon nehéz lesz a fővárost irányítani."[9] Hasonlóan vélekedtek –1993-ban – más törvényalkotók is, sőt volt, aki kereken kimondta, hogy „… nem tartjuk sem jónak, sem pedig életképesnek a fővárosi igazgatás jelenlegi konstrukcióját…" Megfogalmazódott a megoldás is: „…mi azt támogatjuk, amely a fővárosban egy települési önkormányzat létrehozását szorgalmazza. Ez volna a fővárosi önkormányzat egész Budapestre kiterjedő szerepkörrel, a mai kerületekben pedig elöljáróságok működnek..." A szerző még tovább megy, amennyiben egyes fővárosi területrészek leválását is lehetségesnek tartja, illetve a fővárosi agglomeráció és Pest megye helyzetének együttes rendezését is felveti, amely vésősoron Pest megye megszűnésével és egy agglomerációs önkormányzat létrehozásával járna.[10]

A Fővárosi Közgyűlés sem lehetett elégedett a helyzettel, mivel megbízta a főpolgármestert a Fővárosi önkormányzati-közigazgatási rendszerének módosítását célzó tervezet kidolgozásával.[11] Három munkacsoport egymástól függetlenül, kívülről kapott irányelvek (prekoncepció) nélkül készített egy-egy koncepciót.

A három koncepció számos részletben különbözött, egyben azonban egyetértettek: a széttagoltságot meg kell szüntetni, a fővárosi szerepkört erősíteni kell. A tanulmányok címe is

[8] Kiss László: Társulások – kényszertársulások – szervezeti konzekvenciák, In.: A magyar közigazgatás korszerűsítésének elvi és gyakorlati kérdései, oktatási anyag, szerk.: Fogarasi József, UNIÓ Kiadó, 1996.
[9] Sóvágó László: Gondolatok a helyi önkormányzatokról, Magyar Közigazgatás,1993., 43. évf. 11. sz. p. 655.
[10] Böröcz István: Az önkormányzati rendszer fejlesztésének irányai, Magyar Közigazgatás, 1993. 43. évf. 11. sz. p. 668.
[11] Fővárosi Közgyűlés 613-616/1991. sz. határozata

kifejezi ezt a törekvést: „BUDAPEST EGYVÁROS", „AKTÍV KERÜLET, ERŐS FŐVÁROS", „CITY CONCEPCIÓ". Figyelemre méltó, hogy az agglomeráció (Pest megye) helyzetét egyik sem kerülte meg, lényegében a megye területének felosztása került előtérbe.[12]

Új rendezésre váró kérdés – amely a politikai közbeszédben bukkant fel –, egy kistérségi, és (vagy) járási szint (elnevezésében: járás). Ez a területi szint mintegy több száz éven át jelen volt a korabeli helyi önkormányzati és a tanácsrendszerben is. Az első történeti szakaszban, mint a megyei önkormányzatnak alárendelt területi igazgatási szerv működött (járási főszolgabírói hivatal, illetve 1945-től járási főjegyzői hivatal). A tanácsrendszerben már választott testületi szervvel rendelkező területi egységként működött, változó szerepkörrel, döntően a községi vagy járás alá rendelt városok feletti ellenőrző, döntéshozó feladatokkal. 1945-ig legmarkánsabban a községi döntések előzetes vagy utólagos jóváhagyása, felügyelete tartozott ide, a járási főszolgabíró egyben a csendőrség parancsnoka is volt.

A tanácsrendszerben a járási szint nemcsak azzal erősödött, hogy választott testület működött - mint államhatalmi szerv -, hanem a rendkívül alacsony szakmai szinten álló és feladat-hatáskör tekintetében lepusztított községek helyett lényegében ellátta az igazgatási feladatokat (pl.: építésügy, adóügy, szabálysértési ügyintézés stb.), továbbá a mezőgazdasági termeléssel, szövetkezeti gazdálkodással összefüggő feladatok is itt jelentek meg.

A társadalmi-gazdasági helyzet változása következtében a tanácsi feladatok átalakultak járási szinten is, és már a 60-as évek végén kétségessé vált a járások sorsa. Először a járások területe, száma csökkent,[13] majd a feladatok átalakulása és a decentralizáció eredményeként a járási feladatok nagy része megszűnt, következmény: a járások összevonása, majd, mint területi egységek megszüntetése.

A járási egységek megjelenése a helyi önkormányzati rendszerben alapvetően átalakítaná ma is a községi szintű feladatokat és felelősséget, de megkérdőjelezné a megyei szint szükségességét is. Külön probléma, hogy ezen a szinten mennyiben indokolt a képviseleti szerv (testület) létrehozatala, ha ez nem történik meg, akkor pedig az itt megjelenő igazgatási szervezet mely önkormányzati testületirányítása alá kerülne. A társulásos viszony pedig más szervezeti, jogi megoldásokat és feladat- és hatásköri megosztást igényelne. Nem véletlen, hogy ez az egyelőre, - markánsan nem látható - támogatás nélküli politikai elgondolás a levegőben lóg, de nem kizárt az önkormányzati reform keretei közötti megjelenése.

A HELYI ÖNKORMÁNYZATOK TESTÜLETEI

A meghatározó helyi önkormányzati feladatok és hatáskörök letéteményese a választópolgárok által létrehozott testületek: képviselő-testület vagy közgyűlés. A két évtizedes működés során gazdag tapasztalatok halmozódtak fel a testületek létszámát, a testület belső munkaszervezetét és a működési rendet illetően.

A testületi létszám törvényi meghatározása mindig valamilyen társadalmi-politikai nézetrendszer következménye. Már 1990-ben törekvés volt tapasztalható az alacsony létszámú testületek létrehozatalára. Negatívnak ítélték a korábbi tanácsi testületek magas létszámát, azt nem tartották „munkaképes" szervezeti formának, így az 1990-es választásokon létrejött testületek létszáma a korábbinak a harmadára esett vissza. Az utóbbi választásokon (2010-ben) megválasztott helyi önkormányzati képviselők száma tovább csökkent (ugyancsak egyharmaddal).

[12] Síklaky István: Három koncepció a fővárosi önkormányzati reformról, Magyar Közigazgatás,1993. 43. évf. 11. sz. pp. 689-696.

[13] A községek várossá nyilvánításával csökkent egy-egy járáshoz tartozó népesség.

Vélelmezhető, hogy a jelenlegi létszám – legalább is települési bontásban – nem változik, változásra csak akkor lehet számítani, ha a szintek és a struktúrák megváltoznak (pl.: a járások kialakítása, a megyék megszűnése és a régiók létrejötte, a kisközségek önkormányzat-alakítási alapjoga korlátozódik).

A helyi önkormányzati képviselők választásának rendszere stabilnak tűnik, lényegében az elmúlt két évtizedben nem változott. Van azonban néhány olyan kérdéskör, amelyeket érdemes újragondolni és a reform keretében részleteiben is megvitatni. Ezek közül néhányat érdemes - részletes elemzés nélkül- megemlíteni.

A képviseleti gyakorlat is bizonyította, ha a képviselő a település egészéért való felelősségét hangsúlyozza a törvény.[14] Ez esetben az egyéni választókerületek ezzel ellentétes szerepre késztetik a képviselőt, mivel részérdeket kell előtérbe helyeznie. Ezzel összefüggésben, amennyiben marad az egyéni választókerületi mandátum, akkor a képviselő visszahívhatósága merülhet fel.

Az önkormányzati ciklusokat indokolt lenne az országgyűlési ciklustól elválasztani, két éves időközök kialakításával.

Máig tisztázatlan, hogy a képviselők eskütételéhez miért nincs az Ötv.-ben konkrét szöveg, csak az eskü letételéről van rendelkezés.[15]

A választójog feltételezi, hogy az állampolgár (bevándorolt) az adott településen tartós kötelékben éli életét, a közösség sorsáért felelősséget vállaló ember, ki így elvárható, hogy a jog gyakorlása előtt tartósan az adott településen bírjon állandó lakással.[16]

Alapvető kérdéskör az összeférhetetlenségi szabályok újragondolása és eddigi tapasztalatok szerinti szigorítása. A leggyakrabban felmerülő javaslat az, hogy összeférhetetlenségi eset legyen, az illető tartós foglalkoztatási, munkajogi és gazdasági jogviszonyban áll az adott önkormányzattal. Ez a szabály gyakorlatilag kizárná a képviselő-testületből az önkormányzat által foglalkoztatott közalkalmazottat, a vállalkozó orvosokat, az önkormányzati gazdasági társaságok vezetőit. Ezzel elkerülhetővé válna, hogy a képviselő saját egyéb munkáltatói joggyakorlójának a „főnöke” legyen, s hogy az intézményi érdekeke az átfogó települési érdekek fölé kerüljenek.

A választási témakörrel összefüggő összeférhetetlenségi ügy, mindenkinek el kellene dönteni, hogy polgármesteri vagy önkormányzati képviselői mandátumért indul a választáson. A jelenlegi szabályok ezt most megengedik, ezzel gyakori, hogy folyamatossá válik a működési zavar (a politikai kultúra jelenlegi állapotára is tekintettel), a személyes ellentétek háttérbe szoríthatják a települési érdeket.

Abból az elvből kiindulva, hogy a képviselők feladataikat társadalmi megbízatásban látják el, mind gyakoribb javaslat, hogy a képviselői tiszteletdíjak megállapítására ne kerülhessen sor, de a tényleges költségei természetesen kerüljenek megtérítésre. Ezzel visszaszorítható lenne, az un.” megélhetési politikus” kategóriába tartozók száma, amely ma már nem csupán az erős pártpolitikai hatás alatt álló nagyvárosokra és megyékre jellemző, hanem egyre jobban terjed a kistelepüléseken is. A tiszteletdíj eltörlése elősegítené, hogy a helyi közéleti munka

[14] Ötv.19.§ (1) bek.
[15] Ötv.19.§
[16] Több európai államban törvény mondja ki, hogy milyen feltételei vannak a helyi választójognak, pl.: Svédországban a községi önkormányzat tagjai, akik a községben vannak anyakönyvezve, a község területén bármilyen ingatlantulajdonnal rendelkeznek, a községi adót a községben fizetik. Lásd: Szabó Gábor: Önkormányzatok Svédországban, Magyar Közigazgatás, 1990. 40. évf. 11. sz. p. 1043.

becsülete értékkel bírjon, így elsődlegesen azok indulnának a választásokon, akik ténylegesen a közösségért kívánnak tevékenykedni.[17]

A helyi önkormányzati testületek működésével kapcsolatos tapasztalatok azt erősítik, hogy a továbbra is nagyfokú önállóságot indokolt biztosítani az adott viszonyokhoz igazodó helyi szabályozás kialakítása terén, azaz a törvényi kötöttségek körét nem indokolt gyarapítani. A témában megjelent szakmai tanulmányok csak kis számban vetették fel a törvényi módosítás szükségességét. Továbbra is a helyi Szervezeti Működési Szabályzatra (továbbiakban: SZMSZ) érdemes koncentrálni, amelyben a testületen belüli viszonyok, a testületi vezetés, a testületeknek alárendelt szervek irányítását, továbbá a lakossági kapcsolatokat és a társadalmi szervekhez fűződő viszonyt kell meghatározni.

A gyakorlati tapasztalatok rendkívül sokrétűek az egyes települési típusokon belül is (kisközség, község, város, megyei város) és külön kategóriaként kezelhető a megyei szint, valamint a főváros egésze (főváros és kerületek külön-külön is).

A testületek csökkenő létszáma – melynek racionalizálása megkérdőjelezhető – sok vonatkozásban új problémát vetett fel, de ezekre is az SZMSZ nagyobbrészt megoldást adhat. Ilyen vizsgálandó témák:

- a testületi ülések gyakorisága, azok nyilvánosságának tényleges biztosítása;
- az ülést vezető polgármester szerepköre (jogai és kötelezettségei) és a szavazategyenlőség esetén a polgármester szavazata döntsön;
- a bizottsági rendszer korszerűsítése indokolt; a nem képviselőtestületi tagok bizottsági létszámának növelése (törvényi korlát eltörlésével, illetve a mai lehetőségek kihasználásával); a bizottságok működése a képviselő-testületi döntések megalapozottágának és szakszerűségének növelésére és a döntések végrehajtásának ellenőrzésére irányuljon, amennyiben döntési jogkörrel rendelkezik a testület valós kontroljához a feltételeket meg kell teremteni;
- a testületi ülésen résztvevő tanácskozási joggal meghívottak körét az SZMSZ-ben a helyi adottságokra tekintettel szélesíteni indokolt, számukra tényleges megszólalási lehetőséget kell biztosítani.

A polgármester jogállásáról (és az Ötv. vonatkozó részeiről) szóló törvényi szabályozás ésszerű pontosítása több vonatkozásban is felmerülhet. A polgármester a képviselő-testület vezetője, legitimitását egyértelművé teszi közvetlen választásának módja. Gyakorta felmerülő kérdés, a kisközségekben (nevesítve: az ezernél kevesebb lakosú településeken) indokolt-e főállású polgármester foglalkoztatása, a lehetőség biztosítása esetén a település anyagi helyzete, vagy más szempontok legyenek meghatározóak, mint például azok a feladatok, amelyek egy ilyen településen a polgármesteri szerepkörbe utalhatóak (amennyiben arra képesítéssel rendelkezik, vagy vállalja a szükséges ismeretek megszerzését).

Külön vizsgálandó kérdés, hogy a polgármesteri tisztség és a megyei közgyűlési tagság (illetve fővárosi), valamint az országgyűlési képviselőség mennyiben és milyen okokra tekintettel fogadható el a továbbiakban is, vagy összeférhetetlenségi okként lehet kezelni. A megközelítést érdemes lenne érdekképviseleti, érdek-összeütközési s az önkormányzati esélyegyenlőség tekintetében vizsgálni, nem pedig politikai (főleg pártpolitikai) szempontokra figyelemmel. A jelenlegi (megengedő) szabályozás az egyes önkormányzatok közvetlen képviseletét (érdekképviseletét) is lehetővé teszi, míg a többség ezzel a lehetőséggel nem élhet.

[17] Az egyes problémakörök már az Ötv. hatálybalépését követően felmerültek pl.: a Magyar Közigazgatásban már az 1993.évi 13. számban egy tanulmánysorozat jelent meg a helyi önkormányzati törvény továbbfejlesztéséről. Továbbá figyelemreméltó a TÖOSZ javaslata az önkormányzati rendszer továbbfejlesztésére Bp. 2011.

A képviselő-testület és a polgármester kapcsolatának egyik kritikus pontja, hogy a képviselő-testület önfeloszlása esetén megszűnjön-e a polgármesteri megbízatás (ha az Országgyűlés mondja ki a feloszlatást ez a kérdés fel sem merülhet, e polgármesteri tisztség is megszűnik).

Az önkormányzati rendszer 1990.évi kialakításával – több vonatkozásban is – élenjáró ország voltunk a térség rendszerváltoztató országai között. A szakmai irányokkal és azok megoldási formáival sok mindenben azonosult az első demokratikus választáson parlamenti többséget és kormányzati felhatalmazást kapott koalíció.[18] A jelenlegi kérdés az, hogy ebből az élmezőnyből kikerülünk (leszakadunk) vagy jobbak is lehetünk néhány régebbi európai jogállamhoz képest, melynek az az egyik alapfeltétele, hogy a jelenlegi kormányzat helyi önkormányzati rendszer reformjára vonatkozó elképzeléseiben törekedik-e a politikai kompromisszumokon nyugvó megvalósításra.

Felhasznált irodalom

[1] Böröcz István (1993): Az önkormányzati rendszer fejlesztésének irányai, Magyar Közigazgatás, 43.évf. 11. sz. pp. 663-670. HU ISSN 0865-736 X

[2] Jacques Forunier (1997): A megbízható közigazgatás, Magyar Közigazgatás, 47. évf. 10. sz. pp. 631-640. HU ISSN 0865-736 X

[3] Kaltenbach Jenő (1996): Közigazgatás és/vagy önkormányzat, in.: A magyar közigazgatás korszerűsítésének elvi és gyakorlati kérdései,szerk.: Fogarasi József, Unió Kiadó, Budapest.

[4] Kiss László (1996): Társulások-kényszertársulások – szervezeti konzekvenciák, In.: A magyar közigazgatás korszerűsítésének elvi és gyakorlati kérdései, oktatási anyag, szerk.: Fogarasi József, UNIÓ Kiadó, Budapest, pp. 199-201.

[5] Síklaky István (1993): Három koncepció a fővárosi önkormányzati reformról, Magyar Közigazgatás, 43. évf. 11. sz. pp. 689-696. HU ISSN 0865-736 X

[6] Sóvágó László (1993): Gondolatok a helyi önkormányzatokról, Magyar Közigazgatás, 43. évf. 11. sz. pp. 653-655.HU ISSN 0865-736 X

[7] Szabó Gábor (1990): Önkormányzatok Svédországban, Magyar Közigazgatás, 40. évf. 11. sz. pp.1043-1053. HU ISSN 0865-736 X

[8] Szente Zoltán (1994): A helyi területi önkormányzatok alkotmányos szabályozásának elvei, de lege ferenda, Magyar Közigazgatás, 44. évf. 6-7. sz. pp. 364-387. HU ISSN 0865-736 X

[9] Verebélyi Imre (2010): Válságban a magyar középszintű közigazgatás, Új Magyar Közigazgatás, 3. sz. p. 3. ISSN 2060-4599

[10] Waldemar Hummer – Sebastian Bohr: A régiók szerepe a jövő Európájában, Szubszidiaritás-föderalizmus - regionalizmus, Pécs, 1994, pp. 9-56.

[18] Verebélyi Imre: Válságban a magyar középszintű közigazgatás,... ? Új Magyar Közigazgatás, 2010, p. 1.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Balajti István
balajti.istvan@zmne.hu

AZ IKER VHF RADAR STRATÉGIAI JELENTŐSÉGE A MODERN LÉGVÉDELEMBEN

Absztrakt

A robothadviselés nem képzelhető el korszerű és nagyteljesítményű érzékelő rendszer nélkül. A „VHF" vagy ismertebb nevén a „m"-s rádiólokátorok a légtérellenőrzésben jelentkező kedvező tulajdonságai jól ismertek a magyar szakemberek számára. Ezek a képességek egyre inkább felértékelődnek a „lopakodó" technológia és az alacsony pályán tevékenykedő műholdak elszaporodásával. Továbbfejlesztésük igénye vitathatatlan. Ez a cikk az iker VHF radar technológiát és a benne rejlő lehetőségeket mutatja be és néhány a magyar légtérellenőrzés javítását szolgáló fejlesztési javaslattal is hozzájárul a konferencia sikeréhez. Jelen írás a Robothadviselés 11 tudományos konferencián elhangzott előadás írásos változata.

The essential part of the robot warfare is the modern and powerful sensor system. The advanced performances of the VHF or metric wave radars in the air surveillance systems are well-known by the Hungarian experts. These capabilities are more vulnerable today with the increasing number of new types of stealth aircrafts and satellites, which operates at low orbit. The modernization requirements of the VHF radar are indisputable today, but the way of modernization has not been determined yet. This article draws the reader's attention to the twin VHF radar technology and its signal fusion potential benefits. Furthermore, it intends to contribute to the success of the conference with suggestions that could improve the Hungarian air surveillance system efficiency, because the modern twin-VHF-radars should have an increasing role in the modern Air Surveillance Systems. This paper was presented on the 11th Robot warfare scientific conference.

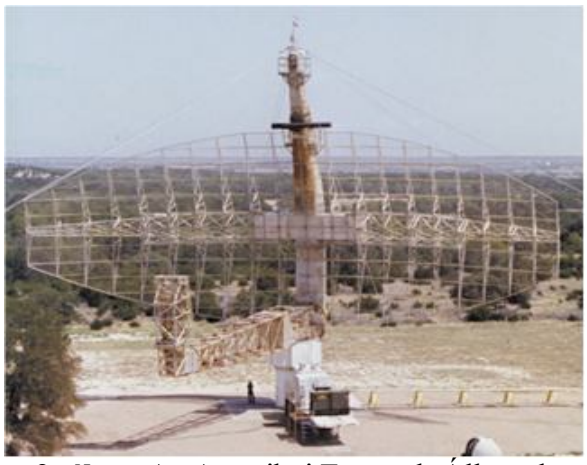
Kulcsszavak: *robothadviselés, légtérellenőrzés, VHF, rádiólokátor ~ robot warfare, air surveillance, VHF, radar*

BEVEZETÉS

A világban számtalan új, korszerű radarokkal és radar rendszerekkel találkozhatunk. A kutatás és fejlesztések is új irányt vettek és a hálózat centrikus elgondolások köré koncentrálódnak. Ezek sorába illik az általam kutatott iker VHF radar technológia.

Az 1. ábra Magyarország közepén üzemelő közepes teljesítményű „m”-es vagy „VHF” radart ábrázol, míg a hozzá nagyon hasonló társa, 2. ábra, az Amerikai Egyesült Állomok Lincoln Laboratórium területén található.

1. ábra. Közepes teljesítményű „m”-es vagy „VHF” radar



2. ábra. Az Amerikai Egyesült Állomok
Lincoln Laboratóriuma területén üzemelő VHF radar

Légtérellenőrzés során három problémát kell megoldani a légtérellenőrzésre kijelölt katonai radaroknak. Ezek:

- az egyre kisebb hatásos radar keresztmetszettel rendelkező repülő eszközök detektálása,
- a detektált, gyakran nagy manőverező kepeséggel rendelkező céltárgyak útvonalba fogása és követése,
- a megbízható azonosítás.

A problémák több ponton párhuzamosan jelentkeznek, melyek közül csak az elmúlt évek legfontosabb irányzataira és a jövőbe mutató tendenciákra hívom fel a figyelmet.

Első helyen kell említeni a *„Lopakodó” képességekkel rendelkező repülő eszközök* terjedését. Napjainkban a passzív módszerek mellett, mint pl. a repülő eszköz alakja, a különböző, az elektor-mágneses hullámokat elnyelő anyagok alkalmazása mellet megjelentek az aktív módszerek is. Ezek közül a legismertebb a néhány éve még „Sci-fi” filmekből ismert

plazma pajzsok térhódítása. Az anyag negyedik állapotát a plazmát alkalmazzák az elektromágneses impulzusok elnyelésére/szétszórására és ez által a repülő eszközök hatásos radar keresztmetszete drasztikusan csökkenthető. A módszer hatékonysága a plazma generátorok teljesítménye és a plazma repülőeszköz felületén történő egyenletes elosztásának lehetőségei jellemezik. Más módszerek kidolgozása és tökéletesítése is folyamatban van, így az optikai és a teljesen digitális elven működő aktív eszközök, melyek a repülő eszköz felületén mért radar impulzusok feszültségével azonos, de ellentétes fázisú jelekkel csökkentik a hatásos radar keresztmetszetet.

A *pilóta nélküli repülő eszközök, drónok,* lehetőségei és fejlődési tendenciái a konferencia központi témája volt és több előadás részletesen bemutatta a megnövekedett hatótávolságban, a felszerelésben megjelenő fegyverzetek komplexitásában és a minimális radar keresztmetszetben rejlő katonai és egyéb lehetőségeket.

Foglalkozni kell a hadszíntéri *harcászati ballisztikus rakéta észlelése* (<1000 km) témakörével, mivel a különböző platformokról indítható, pl. kis és közepes szárazföldi, vízi eszközök száma egyre nő. Megjelentek a csökkentett radar hatásos keresztmetszettel rendelkező megoldások, manőverező képesség és nagyszámú hamis cél, melyek együttesen történő alkalmazása jelentősen kiterjeszti a lehetséges fenyegetettség szintjeit. Az indítási körzet és a célpontok közötti távolság alapján jogos elvárás a távolfelderítő radar rendszerrel szemben, hogy jelezze a támadás irányát és minőségét, még abban az esetben is ha egyenlőre nincs lehetőség a hatékony védelem megszervezésére.

A polgári légirányítás rémálma a *„Nem együttműködő céltárgy azonosítás (NCTR)”,* mivel nem lehet előre tudni, hogy a másodlagos radar rendszerek esetleg a kommunikáció meghibásodásáról, vagy talán egy terrorfenyegetettségről van szó.

Napjainkra a légtér fenyegetettsége kiegészül az *alacsony pályán,* 80-500 km *megjelenő műholdakkal,* melyek mint nagyteljesítményű zavaradók és kommunikációs feladataik révén mint a cyber támadások eszközei is lehetnek. Ez a fenyegetettség, mint kategória annyira komoly, hogy az ellene való védelem teljesen új radar rendszer kiépítését feltételezi.

Ezek a régi/új fenyegetettségek új típusú védelmi rendszerek, módszerek és radarok kidolgozását igénylik, mely kihívásnak a magyar szakemberek is megpróbálnak megfelelni. Erre a radarokkal kapcsolatos történelmi hátterünk is feljogosít minket.

MAGYAR TÖRTÉNELMI TAPASZTALATOK

A radarfejlesztéssel foglalkozó tudósok sorát Jáky József ezds. (1897-1945) nyitja, aki Magyarországon, az 1930-as években felismerte a rádiólokációban rejlő lehetőségeket. Ő a “Sas", “Borbála”, “Bagoly” és a “Turul rádiólokátorok harcászati-műszaki követelményeinek megfogalmazásával, a témák elindításával biztosította, hogy hazánk a II. világháború végére csatlakozott a radargyártó nemzetekhez.

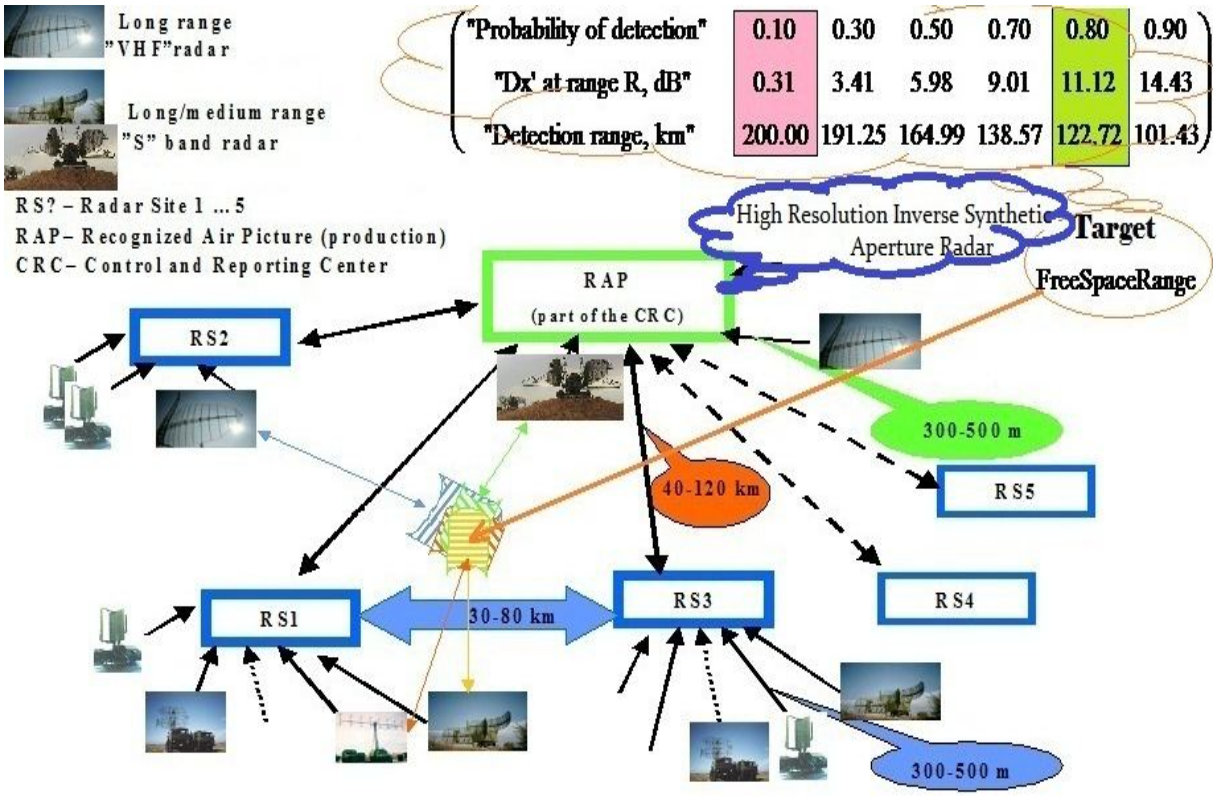
A „Sas” radar műszaki megvalósításával Bay Zoltán Lajos (1900-1992) örökre beírta nevét a magyar és nemzetközi radar történelembe, hiszen a 1946. februárjában az amerikai „Diana” projekttel egyidőben kísérletezett a Holdról visszaverődő radar impulzusok összegyűjtésével, felfedezve a jelintegrálást.

A Kálmán Rudolf Emil, (1930-) által alkotott "Kalman Filter” nélkül ma szegényebb lenne a repülő és rakétatechnika, valamint a radarjelentésekre épülő korszerű útvonalképzés.

Dénes Gábor (1900 – 1979) a mikrohullámú holográfia megalkotásával lehetőséget biztosított a fázisvezérelt rácsantennák hibáinak pontos behatárolására és a radar képalkotó módszerek tökéletesítésére.

Neumann János (1903 - 1957) jelentős szerepet vállalt a nagysebességű számítógépek megalkotásában és társszerzője a napjainkra oly fontos játékelméletnek.

A 3. ábra magyar radar zászlóalj struktúrát ábrázol az 1980-s évek végéről. A részletek értékelése nem fér bele a cikk terjedelmébe, de néhány napjainkban is korszerűnek számító megoldás mindenképp említést érdemel. A legfontosabb a hálózat centrikus radar adatfeldolgozás, melyben a célok detektálása fix és mobil telepítésű „VHF”, L” és „S” sávú radarok alkotta nagy átfedési együtthatóval rendelkező rendszerrel történt. Az akkoriban legkorszerűbbnek számító radarok esetén lehetőség volt a különösen fontos irányokban, több egymással párhuzamosan futó „küszöb” szint alkalmazására, melynek segítségével a kis hatásos visszaverő felületekkel rendelkező, vagy manőverező céltárgyak detektálása és útvonalba fogása is biztosítható volt. Elméleti lehetőségeit a 3. ábra jobb felső sarkában található táblázat bizonyítja. Ha adott körülmény között a céltárgy detektálás valószínűségére vonatkozó elvárás 0.9, akkor az ehhez szükséges jel-zaj(zavar) viszony 14.43 és a radartól 101km-re detektálható. A detektálás valószínűségére vonatkozó elvárás csökkenésével a szükséges jel-zaj(zavar) viszony is csökkenthető, és ezáltal a céltárgy detektálásának távolsága növelhető, így 0.1 érték esetén a céltárgy felderítési távolsága már 200 km. Természetesen a vaklárma valószínűségek jelentős növekedése mellett. A rendszer hátránya bonyolultságából fakadt, hiszen üzemmérnöki szintű mérnök-műszaki állomány kellett az üzemeltetéséhez, ezért a kiképzés és a logisztikai támogatás rendkívül költséges volt. Külön ki kell emelni a szigorúan tikosan kezelt és csak egy zászlóalj harcállásponthoz csatolt nagyfelbontású inverz szintetikus apertúra elven üzemelő radart, mely 18 KHz sávszélességgel néhány Hz felbontás pontosan képezte a célokról visszavert spektrum képeket.



3. ábra. Zászlóalj szintű radar rendszer a 1980-as évek végén

A 4. ábra egy magyar MI-17 helikoptert és a lebegést biztosító rotorok sebességkomponenseinek spektrumát mutatja, melyet a nagyfelbontású inverz szintetikus apertúra radar szolgáltatott. Természetesen a valóság ennél „árnyaltabb” mivel ez a helikopter

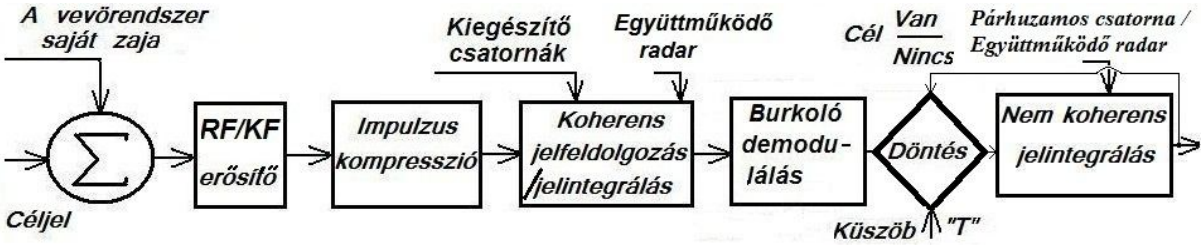
aktív fázisrács antennákkal van felszerelve, és ha szükségét „érezte” aktív zavarással képes volt „átrendezni” a spektrumképet.

4. ábra. MI-17 helikopter és a nagyfelbontású inverz szintetikus apertúra radar spektrumképe

HÁLÓZAT- CENTRIKUS MEGOLDÁSOK KOHERENS JELFELDOLGOZÁSSAL

Napjainkra a számítástechnikai eszközök/hálózatok fejlődése nem kíván magyarázatokat. Általuk a legbonyolultabb elképzelések is aránylag olcsón megvalósíthatók, „csak” tudnunk kell mit, miért és hogyan?

Az 5. ábra egy koherens jelfeldolgozásra optimalizált radar vevőrendszer általános sémája. Valószínűleg Bay Zoltán volt az első, aki megállapította, hogy a rendkívül kis jel-zaj(zavar) viszonnyal rendelkező céljelek koherensen integrálhatók és ezáltal a jel értéke négyzetesen, míg a zaj értéke „csak” lineárisan nő, hiszen a vet jelek fázisa és amplitúdója is ismert, szemben a zaj jelekkel, melyek fázisa véletlenszerűen változó. Ezt az eljárást detektálás előtti jelintegrálásnak is nevezik, szemben a nem koherens jel integrálással, mely a cél van/nincs döntőáramkör után helyezkedik el.



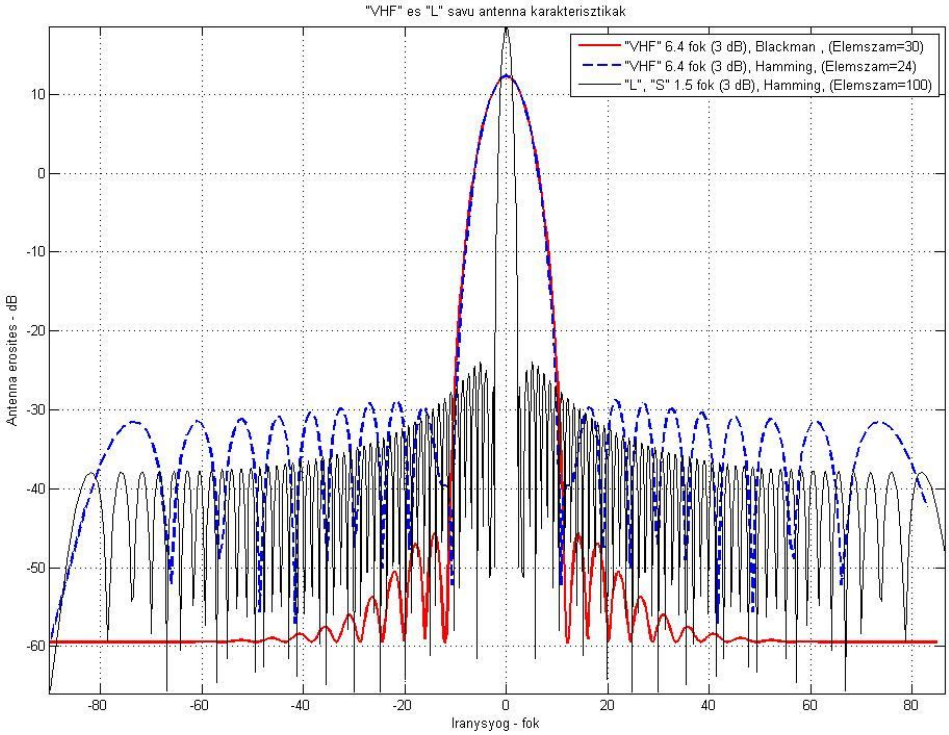
5. ábra. Koherens jelfeldolgozásra optimalizált radar vevőrendszer

Ismert bár nem eléggé hangsúlyozott tény, hogy koherens jelintegrálással a hasznos jel a zavaró jelek alól is kiemelhető, ezáltal a radarok zavarvédelme jelentősen növelhető. Az aktív és passzív zavarvédelem különösen akkor lehet hatékony, ha az adójel alakja a harchelyzethez alkalmazkodva változtatható.

A koherensen jelfeldolgozás fő hátrányaként említik a vett jelek fázisérzékenységét, mely sok tényező függvénye. A fázishibák leglényegesebb elemei a repülő eszköz mozgása okozta doppler, a hullámterjedési rendellenességek és a párhuzamosan futó vevőrendszerek korrelációs tényezőire vonatkozó elvárások, melynek jobbnak kell lennie, mint 0.99. Ennek következtében megvalósításuk sokkal drágább, mint a nem koherens jelfeldolgozással rendelkező radaroké.

A VHF ÉS AZ L/S SÁVÚ RADAROK ELŐNYEI ÉS HÁTRÁNYAI

A rádiólokátorok antennarendszereinek iránykarakterisztikái, mint a feladatra optimalizált legtökéletesebb térbeli szűrők funkcionálnak. Legfontosabb paraméterük a fél teljesítményen mért fő nyalábszélesség és az oldalnyalábok szintje. Az oldalnyalábok szintje megfelelő ablak függvények alkalmazásával csökkenthető. Természetesen kompromisszumokon alapuló tervezési feladat, adott elemű antennaméretekhez az elvárt oldalnyaláb szint és fő nyaláb szélesség eléréséhez szükséges bonyolultságú ablakfüggvény gyártástechnológiai realizálása. A 6. ábrán két lehetséges megoldás szimulációs eredményeit mutatom be.



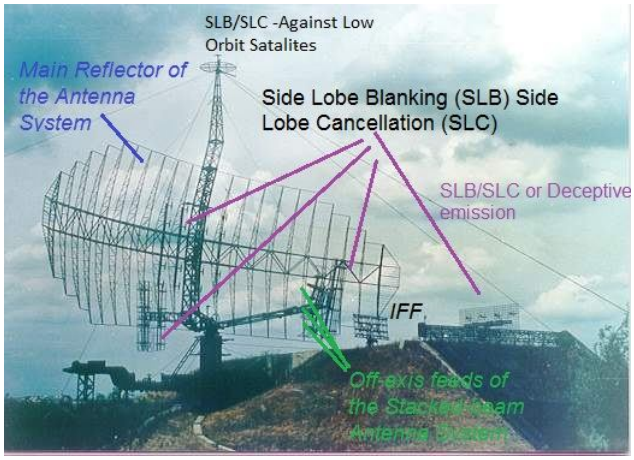
6. ábra. VHF, L és S sávú antenna iránykarakterisztikák

Gyakorlati tapasztalatokkal bizonyított, hogy az 1.5 fokos főnyaláb szélesség a légtér ellenőrzési feladatok ellátására megfelelő mérési pontosságot ad. Ezért kiszámítottam, hogy megvalósításához, a 45 dB oldal nyalábszintet biztosító Hamming ablakfüggvény 100 elemű fázisrács antenna alkalmazásával, a különböző hullámsávban üzemelő antennák mérete milyen nagyságú. Az antenna elemek egymáshoz viszonyítva fél hullámhosszra helyezése esetén az *„S”* sávban (3.1 GHz) a szükséges antennaméret *4.84 m,* míg az *„L”* sávban (1.3 GHz) ez már *12.54 m*, míg a *„VHF”* sávban (180 MHz) az antennaméret *83.3m*. 84 m-s antennák építése és üzemeltetése költséges, ezért gyakorlati tapasztalatok alapján a VHF sávban megengedhető a főnyaláb antenna szélességének 6-6.5 fokra növelése. Ennek megvalósítása már egy 20 m-s 24 elemű antennával lehetséges kb. 40 dB-s oldalnyaláb szintekkel. Ha az oldalnyaláb szintet 50 dB alá csökkentjük, ahogy a 6. ábra mutatja, akkor legalább 30 antennaelemet tartalmazó 25 m-s antennát kell készíteni a bonyolultabb Blackman ablak függvény realizálásával.

Ezekből a paraméterekből következik az L és S sávú radaroknak a VHF radarokkal szembeni nagyobb szögmérési pontossága. Mivel a hullámhossz csökkenésével az antenna méretek is csökkennek, így az L, S sáv és magasabb frekvenciatartományok alkalmasabbak többfunkciós, többcélú radarok készítésére, mely radarok nélkülözhetetlenek a hadihajók és

repülőgépek fedélzetén. Ezekben a frekvencia tartományokban viszont csak rendkívül költségesen, extrém nagy teljesítményekkel és antennákkal, oldható meg a „lopakodó" technológiával rendelkező repülő eszközök detektálása és rendkívül sebezhetőek az olcsó önrávezető rakéták által. Általában problémás a manőverező földközeli célok detektálása többszörös hullámterjedés és romló időjárási körülmények esetén. Ezzel szemben a „VHF" radarok jól megválasztott települési hely esetén képesek kihasználni a többszörös hullámterjedés teljesítménynövelő hatásait és az időjárási körülmények változására sokkal kevésbé érzékenyek. Számukra csak az *aktív a „lopakodó" technológiával* rendelkező repülő eszközök detektálása problematikus. A már rendszerben lévő VHF radar főbb antenna jellemzőit mutatja a 7. ábra

Napjainkban valamennyi új radar beszerzése illetve modernizálása megköveteli a cyber védelem és az alacsonypályán tevékenykedő pl. zavarást alkalmazó műholdak elleni védelem kidolgozását. Ugyanígy gyakran problémás a vezetési rendszerrel nem együttműködő eszközök azonosítása.



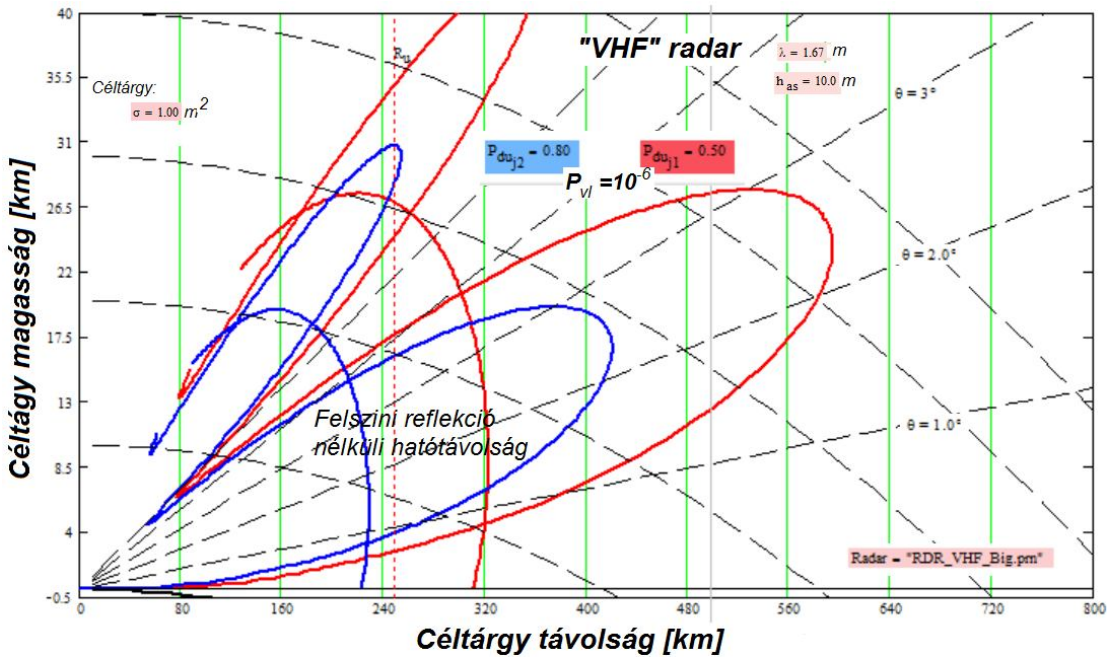
7. ábra. VHF radar antenna jellemzők

A fő antenna mérete vízszintesen és függőlegesen valamivel több, mint 32x11 m. Az antenna tetején a műholdakról történő zavarás elnyomására szolgáló oldalnyaláb kompenzáló- és zavar impulzusok blokkoló segéd antennarendszer látható. A jobboldalon látható lefogó antenna több funkciót is elláthat. Együtt forogva a fő antennával, általános zavarás esetén, egy az adaptív zavarszűrők (lila vonallal jelölt antennák) bemeneteinek. Nagyon intenzív zavarás esetén követi a zavaró adót és maximalizálja a zavarás elleni védelem hatékonyságát. Önrávezető rakéta észlelése esetén üzemmód váltás történik és a radar főantennájáról az adójel teljesítménye ide kerül átirányításra, hogy csaliként védje a főantennát.

MODERN FÁZISVEZÉRELT VHF RADAR KONCEPCIÓ

Napjainkban az antenna rendszer méreteinek csökkentésére és a radar performanciák lehetőségeinek növelésére a VHF frekvencia sávban is fázisvezérelt antennák elterjedése tapasztalható. A 6. ábrán látható kb. 23 m-s antenna rendelkezhet az alábbi paraméterekkel.

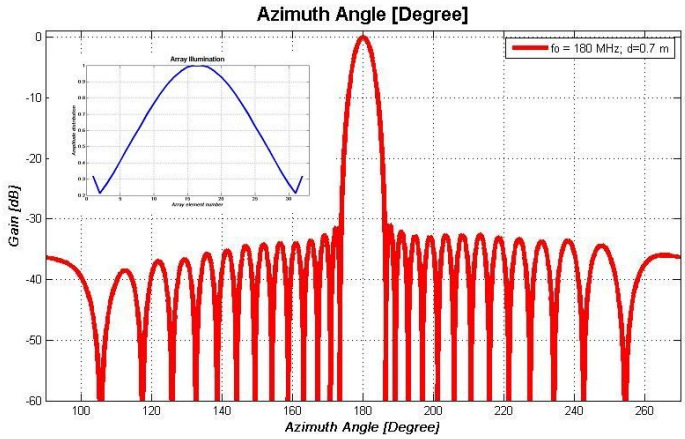
A fázisvezérelt antenna adási nyeresége legyen 23.5 dB cosec^2 függőleges iránykarakterisztikával, míg a 7 darab vételi legyezőnyaláb erősítése 27.5 dB. Az adórendszer átlagteljesítménye 2.25 kW. A radar többi performanciája: érzékenység, sávszélesség, veszteségek stb. olyan toleranciával készülnek, hogy megfeleljenek a 8. ábra céltárgy detekciós elvárásainak (P_d=0.8 és 0.5, $P_{vl}=10^{-6}$ Sw1 típusú 1 m^2 RCS). Az antenna rendszer földfelszíntől mért középpontjának magassága 10 m és a radar vivőfrekvencia 180 MHz.



8. ábra. Közepes teljesítményű VHF radar céltárgy detekciós lehetőségei

8. ábra Az ábrán jól megfigyelhető, hogy a földfelszín okozta reflekció következtében a függőleges irány karakterisztika felszakadozik és a radar céltárgy detektálási lehetőségei 2.5 foknál 427 km-re nőnek szemben a szabadtéri 235 km-s hatótávolsággal. A 4.5 foknál látható, és magasabb helyszögeken ismétlődő beszívások kiküszöbölésére frekvencia diverzió alkalmazható fázisrács antennák esetén. Az ábra jól szemlélteti a két párhuzamosan alkalmazott küszöb szintek, P_d=0.8 és 0.5, P_{vl}=10^{-6} értékekre meghatározva, nyújtotta céltárgy detektálásban jelentkező előnyt.

A 9. ábra a 32 dipól sugárzót tartalmazó fázisrács antenna oldalszög irány karakterisztikáját mutatja egy egyszerűen megvalósítható amplitúdó eloszlásfüggvénnyel. Mivel nem elvárás a nyaláb elektromos mozgatása, ezért az egymástól 0.7 m-re helyezett sugárzók szimmetrikusan csatlakoznak az adás-vétel csatolóhoz.

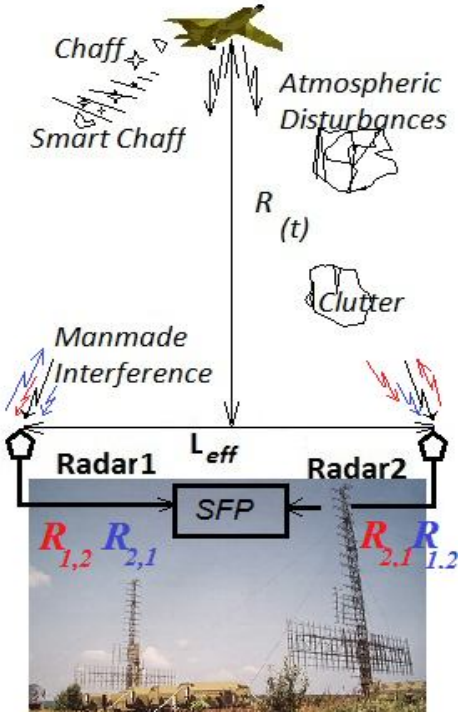


9. ábra. A fázisrács antenna oldalszög irány karakterisztikáját

Jól látható, hogy ez az egyszerű megoldás 6-6.5 fokos félteljesítményű irány élességi szög mellet jónak számító 30 dB-s oldalnyaláb szintet, biztosit, mely adaptív szűrési technikák alkalmazásával tovább csökkenthető.

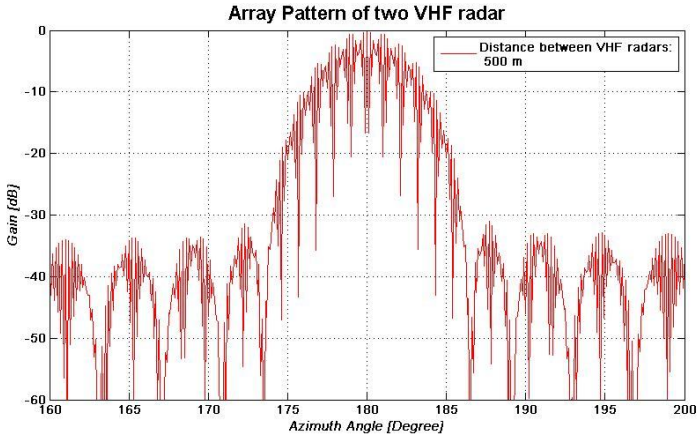
AZ IKER VHF RADAR KONCEPCIÓ

Ismert, hogy a radar rendszerek jelfeldolgozása felosztható térben nem koherens, rövid ideig térben koherens és térben koherens esetekre. Napjainkban a térben nem koherens estek: a polgári légi-irányítás által használt útvonal egyesítés, a katonai vezetési rendszerekben elterjedt plot-plot koreláltatás és a 3. ábra eszközrendszerében is szereplő videó-jelegyesítés lehetnek. Ezzel szemben az igazán korszerű megoldások csak az RF-jel koherens integrálását és az ehhez szorosan kapcsolódó plot-plot egyesítést alkalmazzák. Az Iker VHF radar koncepció a két utóbbi megoldást ötvözi, egy olyan bi-statikus radar rendszer elrendezésben, ahol a közepes hatótávolságú VHF radarok, 9.ábra leírása, egymáshoz viszonyított távolsága, L_{eff}, csak néhány száz méter. Ezt szemlélteti a 10. ábra.



10. ábra. Iker VHF radar rendszer

A 10. ábra fényképe két Nyebo típusú VHF radart ábrázol (mely feltételezésem szerint) iker VHF radar üzemmódokban képes működni. Mindkét radar nemcsak a saját kisugárzott impulzusait képes venni és koherensen feldolgozni, de a mellette levő másik radar jeleit is. A 10. ábrán piros és kék nyilakkal jelzett villámok, valamint az autókorrelációs függvényeket jellemző R_{xy} jelzések ezt szemléltetik. A két antenna egymással szinkronban forog, indító- és szinkronjeleik, valamint jelfeldolgozásuk az SFP-vel jelzett jelfeldolgozó központban kerül kidolgozásra illetve megvalósításra. Az ábrán megfigyelhető környezeti hatások általánosnak tekinthetők egy katonai rádiólokátor számára. A legnagyobb problémát a két radar antennarendszereinek egymásra hatása képezheti, mely az antennák elmélete szerint a főnyalábok felszakadozásában nyilvánul meg. E hatás ellenőrzésére kiszámítottam két egymástól 500 m elhelyezett a 9. ábrán bemutatott iránykarakterisztikával rendelkező VHF antennarendszer egymásra hatását. A számítási eredményeket a 11. ábra jeleníti meg.

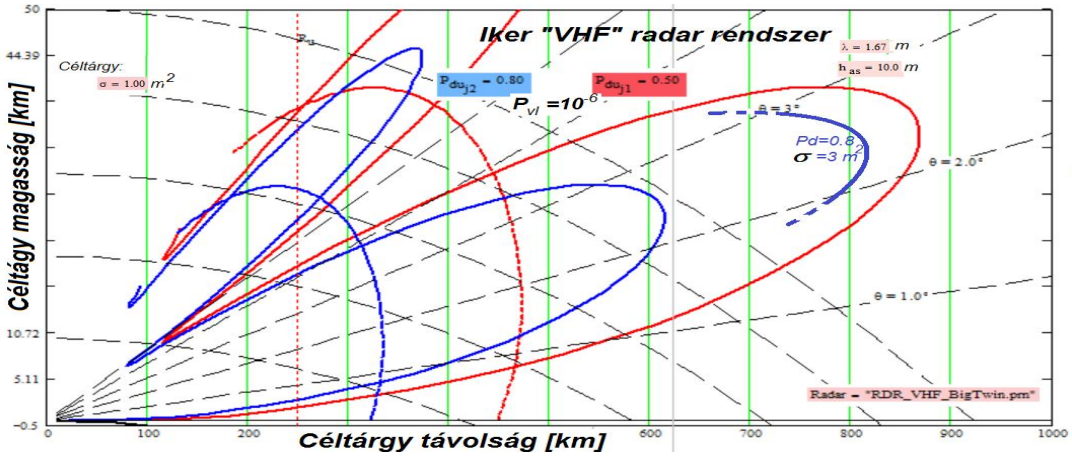


11. ábra. Két egymástól 500 m elhelyezet VHF antenna iránykarakterisztikája

A főnyalábot több jelentős 20 dB beszívás jellemzi, mely jelentősen modulálhatja a céltárgyakról visszavert jelet. Ugyanakkor a főnyalábon jelentkező beszívások helye pontosan meghatározható illetve számítható. Ez a jelenség úgy működhet, mint toló lécen a nóniusz skála, a beszívások számának mértékében pontosítható a szögmérési pontosság. Más frekvenciákon a beszívások helye máshova kerül, így frekvencia diversity üzemmódban a beszívások miatti jelveszteség kompenzálható.

Az Iker VHF radarok előnyei/kihívásai

Változatlan adóteljesítmény mellett a céltárgy detekciós lehetőségek növekednek legalább 40 %-kal, mivel a közös antennák miatt az antennaerősítés úgy adásra, mint vételre 3 dB-lel megnő. $P_{átlag}$=2.25 kW; G_T=26.5dB; G_R=30.5dB, paraméterekkel a Sw1 típusú 1 m^2 cél a 12. ábra szerint detektálható (3 m^2 cél esetén R_{max}= 817 km-re növekszik. Ismert, hogy ugyanaz a céltárgy a VHF frekvencián 5-10 dB- lel nagyobb hatásos radar keresztmetszettel rendelkezik, mint az L (D) sávban.)



12. ábra. Iker VHF radar rendszer céltárgy detekciós lehetőségei

Összehasonlítva a 8. 11. és a 12. ábra eredményeit megállapítható, hogy az iker VHF radar koncepció további előnye a radar megnövekedett:

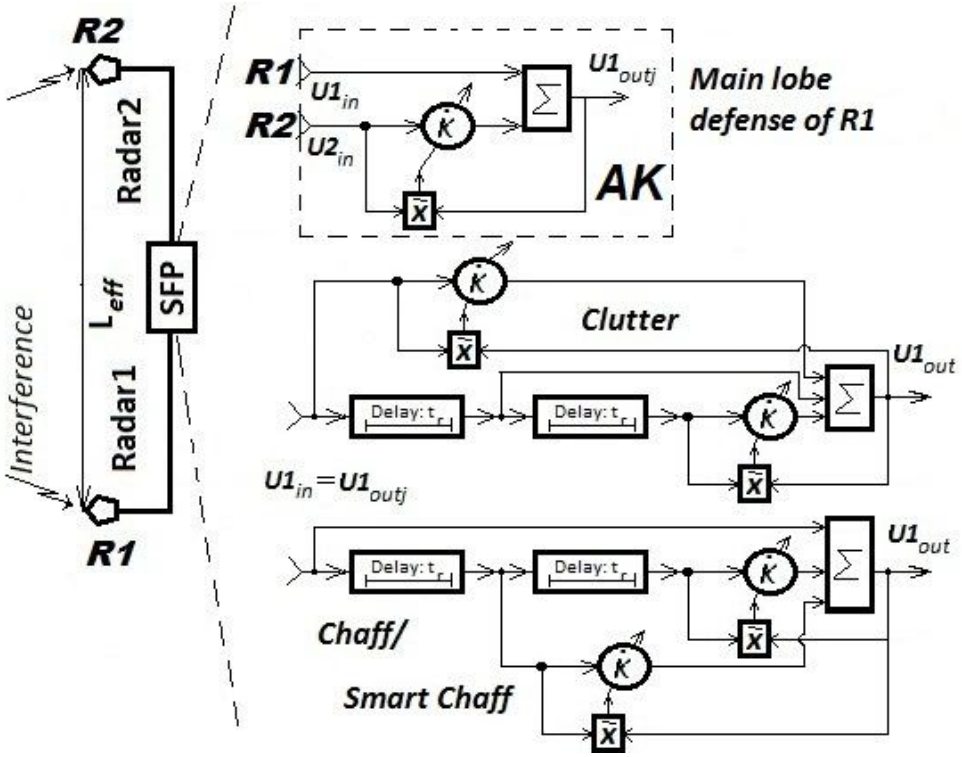
- Felbontása
- Mérési pontossága
- Útvonalképzés / illetve fenntartási képesség
- Álló cél és aktív zavarvédelem
- Túlélőképesség és rendelkezésre állás

- Új katonai felhasználási terület pl: Passzív koherens lokáció a Föld-Levegő-Föld és a Levegő-Levegő kommunikáció beazonosítására illetve ha szükséges zavarására.

Ahhoz, hogy az előnyöket kihasználhassuk, meg kell oldani a VHF radarok és a központ:

- Teljes központi vezérlését.
- Egyesített koherens jelfeldolgozását.
- Az adójelek üzemmód függő fázis szinkronizálást a különböző antennákon.
- A térletapogatás irányában is változó paraméterek beállítását illetve pontosítását.
- A közös aktív és passzív zavarvédelemhez és jelfeldolgozáshoz szükséges korrelációs együttható értékek magas szinten tartását.
- A számítástehnikai hálózat centrikus HW & SW teljesítmény követelmények teljesítését.

A 13. ábra az iker VHF radar koncepció zavarvédelmi képességeit szemlélteti. Az egymástól függetlenül is működtethető VHF radarok rendelkeznek mindazon aktív védelmi berendezésekkel, antennák és adaptív szűrőkkel, melyek már a 7. ábrán áttekintésre kerültek. Ugyanakkor a korszerű fázisvezérelt antennák alkalmazása lehetőséget biztosit a realizálás hatékonyságának növelésére, hiszen a nagy fázisvezérelt antenna felület feloszthető elemi antenna rendszerekké, melyek az elvárások szerint konfigurálhatóak az adaptív szűrők bemenetére. A megnövekedett flexibilitás és az új digitális jelfeldolgozás következtében a rendszerek korrelációs tényezői magasabb szinten realizálhatók, mint ami a 7. ábrán megvalósított berendezésekkel elérhető. További előnye az iker VHF radar koncepciónak, hogy az adaptív szűrők hatásfokának javítására további elvi és gyakorlati lehetőségeket kínál. Ezek közül kiemelendő a főnyaláb védelme, melynek megvalósítása a 13. ábra felső részen látható. Ez egy olyan adaptív szűrő, ahol a bemeneti jeleket, a fő és a kisegítő csatornák számára elvben teljesen azonos antennák szolgáltatják. Mivel a csatornák erősítése, minden irányban nagyon hasonló, az adójel spektruma pontosan ismert, a zavaró adók iránya nagy pontossággal adaptívan meghatározható és az általuk injektált interferenciák nagy zavarelnyomási tényezővel szűrhetők.



13. ábra. Zavarvédelmi eszközök

További előnye a zavarvédelemnek, hogy a 7. ábrán bemutatott radarban már jól bevált, a célra vagy a passzív zavarra fókuszált, úgynevezett *külső koherens* üzemmód szintén adaptív szűrőkkel csökkenti az állócélok és egyéb passzív zavarok céltárgy detektálást rontó hatását. Erre a feladatra a radar kisugárzási ismétlődési frekvenciára szimmetrikus késleltetéssel rendelkező adaptív szűrők a leghatásosabbak. Bonyolult légi helyzetben, dipólfelhők alkalmazása esetén, amikor a széljárás turbolenciákkal szélesíti a visszavert jelek spektrumát az asszimetrikus késleltető vonalakkal ellátott adaptív szűrők hatásfoka jobb. Külön előny, hogy napjainkra a helyzethez legjobban adaptálható szűrési algoritmusok könnyen és egyszerűen integrálhatók a teljesen digitális jelfeldolgozásba.

Észre kell vennünk, hogy az iker VHF radar rendszer lehetőségei megnövekedtek a passzív zavarvédelem területén, hiszen a két antenna, két különböző frekvencián tapogatja le a teret, de az ismétlődési frekvencia azonos, az önálló antennákra érkező jelek fázisfutás különbsége pontosan számítható illetve mérhető, valamint a célokról és passzív zavarokról kétszer több információ áll rendelkezésre, mint pl. a 7. ábrán bemutatott radar esetén.

KÖVETKEZTETÉSEK

A fentiek alapján megállapítható, hogy az iker VHF radarok stratégiai jelentősége:

- a céltárgy detektálási képesség növekedésében,
- a felbontóképesség és mérési pontosság növekedésében,
- a megnövekedett zavarvédelmi képességekben,
- a kiterjeszthető széles spektrum következtében megnövekedő információszolgáltatás képességben,
- a megnövekedett doppler sebesség mérési pontosság miatt a céltárgyak útvonal indítása ás fenntartási valószínűség növekedésben, valamint,
- a radar rendszer megnövekedett túlélőképességében, megbízhatóságában és rendelkezésre állóságában jelentkezik.

Ezen előnyök biztosításához teljes koherens jelfeldolgozás szükséges, melynek megvalósítása a VHF frekvenciasávban a legkönnyebb. Számításokkal igazolható, hogy az iker VHF radar rendszer alacsony költségekkel realizálható.

Ezek figyelembe vételével javasolt:

- A magyar VHF radarok korszerűsítésének folytatása
  - Új VHF antenna típusok kidolgozása (e.g. a P-18M antennák lecserélésére);
  - A kommunikációs cégek által sokat hangoztatott MIMO technológia integrálása a VHF radar rendszerbe;
  - A legkorszerűbb jelfeldolgozási módszerek, neutrális hálózatok, optikai jelfeldolgozás integrálása, nem csak az iker VHF radarokba, de a hozzájuk szorosan kapcsolódó radar képalkotási projektekbe;
  - Az iker VHF radarok további harctéri alkalmazási lehetőségeinek kutatása.
- A VHF frekvencia tartomány európai kijelöléséhez szükséges lépések megtétele.
- Elméleti kutatások indítása az iker VHF radarok hologram képzési lehetőségeivel kapcsolatban
- A 14. ábrán bemutatott iker VHF radarral kapcsolatos adatgyűjtés folytatása.

14. ábra. Iker VHF radar koncepció hagyományos hardvereken

Felhasznált irodalom

[1] Dr. V. Chernak: Tutorial at the Radar 2010 Conference held in Arlington, VA, USA on 10th May 2010. ISBN-13: 9789056991654 (For Nebo radar see: http://www.rusarmy.com/pvo/pvo_vvs/rls_nebo.html)

[2] Dr. V. Chernak : Fundamentals of Multisite Radar systems, Gordon & Breach Science Publisher, 1998; ISBN-10: 9056991655 ;

[3] D.K.Barton: Modern Radar System Analysis ver 3.0 Software and User`s Manual, Artech House, Inc. 2007. ISBN 13:978-1-59693-264-7

[4] Microwave Journal, Metric Radars Win Reprieve in Hungary, June 1, 2006, http://www.mwjournal.com/Journal/?Id=25

[5] Zsolt Haig: Connections between cyber warfare and information operations, Vol. 8, No. 2 (2009) 329–337, ISSN 1788-0017

[6] Kuschel, H.; Heckenbach, J.; Muller, S.; Appel, R.: On the potentials of passive, multistatic, low frequency radars to counter stealth and detect low flying targets, Radar Conference, 26-30 May 2008

[7] Seller Rudolf: Módszerek céltárgyparaméterek rádiólokációs mérési pontosságának növelésére, Egyetemi doktori értekezés, BME, Budapest 1996

[8] Ványa László: Elektronikai Hadviselési Állomás fejlesztése szoftverrádió technológiával – Az Interjam projekt. Kommunikáció 2009 tudományos konferencia kiadványa, Budapest, ZMNE, 2009

[9] Haig Zsolt – Kovács László: Műholdas távközlési rendszerek. Az informatikai biztonság kézikönyve. Verlag Dashörfer Szakkiadó Kft. Budapest 2008.

[10] Gy. Kende, Gy. Seres: The use of chess in military matters, Akademia Obrony Narodowe, Zeszyty Naukowe 2007/1, Waraszawa, 412-424.p

[11] K. E. Olsen, K. Woodbridge, ”Performance of a Multiband Passive Bistatic Radar Processing Scheme - Part I”, IEEE AES System Magazine (AESSM) Special Issue on Passive Coherent Location, invited paper submitted 31. August 2011.

[12] Yngve Steinheim: Blake Chart with EXCEL program, received by e-mail,

[13] H. Kuschel: VHF/UHF radar. 1. Characteristics, Electronics & Communication Engineering Journal, Apr 2002, Volume: 14 Issue: 2, page(s): 61 – 72, ISSN: 0954-0695

[14] Hajdú Ferenc: In memoriam Dr. Jáky József, Az első magyar, aki rádiólokátort látott? Élet és tudomány, 2011/24.

[15] Péter Renner: The role of the Hungarian engineers in the development of radar systems, Periodica Polytechnica, SER. SOC. MAN. SCI. VOL. 12, NO. 2, PP. 277–291 (2004)

[16] Bálint Kunos: Defence economy and the European Union. Tradecaft Rreview(Special Issue), Budapest, Hungary 2010

[17] Végh Ferenc: Magyar Honvédség feladatai és struktúrája az ezredforduló után, a biztonság alakulásának függvényében: doktori (Ph.D.) értekezés, Budapest, ZMNE, 1999

[18] Balajti István: Korszerű katonai radarok és radaradat-feldolgozó rendszerek, Egyetemi Jegyzet, Budapest: ZMNE, 1998, 275 p.

[19] Balajti István: Az iker VHF radar elképzelés menedzselésével kapcsolatos kérdéskör, Előtanulmány, Robothadviselés, Tudományos konferencia, 2011. November. 24, Budapest

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Balajti István
balajti.istvan@uni-nke.hu

AZ IKER VHF RADAR ELKÉPZELÉS MENEDZSELÉSÉVEL KAPCSOLATOS KÉRDÉSKÖR
(ELŐTANULMÁNY)

Absztrakt

A projekt menedzselés hatékonyságának növelése minden robothadviseléssel kapcsolatos tevékenység központi kérdése. Ezek a képességek egyre inkább felértékelődnek, hiszen a kis és nagy beruházások sikere és kudarca alapvetően az azt megvalósító vezetők hozzáértésének függvénye. Az ehhez kapcsolódó kérdéskör, különösen, ha nemzetközi kitekintésre is lehetőséget nyújt, elengedhetetlen a szakemberek képzéséhez. Ezért az alkalmazható módszerek továbbfejlesztése állandó folyamat. A cikk az iker VHF radar technológia menedzselésével kapcsolatos kérdéskör vizsgálatán keresztül mutatja be a speciális IT mintaprojektek indításával kapcsolatos elvárásokat: melyek a követelmények és kockázatok felmérése; a lehetséges problémák számbavétele; az aktuális vagy javító tevékenységek; az események projekt tartópillérek szerinti értékelése és a célkitűzések elérése valószínűségének összefoglalása. Jelen írás a Robothadviselés 11 tudományos konferencián elhangzott előadás írásos változata.

The project management efficiency is the key measure of the activities related to Robot-warfare, because it determines the capability of the leaders to be successful dealing with small or big projects in achieving the development objectives. All relevant information on the project implementation and progress are very important for the students' education, especially if it has international relations as well. We can see that all the currently in-place-applied project management methodologies are under a permanent modernization. This article focuses on the twin VHF radar management aspects and highlights the performance assessments for twin VHF radar Pilot Project supervision: the key assumptions and risks; the major problems encountered; the actual or proposed remedial actions; and the project legs ratings for implementation progress and the likelihood of achieving development objectives. This paper was presented on the 11th Robot warfare scientific conference.

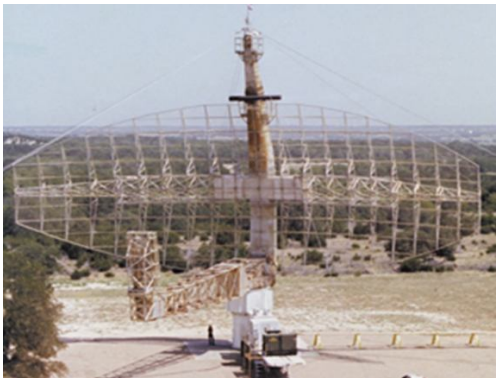
Kulcsszavak: *projektmenedzselés, robothadviselés, VHF radar ~ project management, VHF radar, robot warfare*

BEVEZETÉS

Napjaink projekt menedzselése jelentős változásokon megy keresztül. A régen ismert és gyakorolt módszerek mellet egyre inkább előtérbe kerülnek a nemzetközi projektek, melyek sikere vagy éppen kudarca nagymértékben attól függ, mennyire vagyunk képesek felmérni a környezetet ahol a projekteknek meg kell valósulnia és megérteni a velünk egy projekten dolgozók elvárásait, gondolkozásmódját. Ennek ismeretében könnyebben próbálhatjuk meg lehetőleg sikeresen, saját és nemzeti érdekeinket érvényesíteni. Bár igaz, hogy általában a nemzetközi projektek menedzselése rendkívül összetett tevékenységek halmaza és nagymértékben függ a különböző emberek tudás szintjétől, mégis célszerű az új projektek indítása előtt áttekinteni, illetve felmérni az induló projekt főbb összetevőihez tartozó elvárásokat, a rendelkezésre álló vagy szükséges erőforrások nagyságát a feladatok megoldásához szükséges időtényezőt és elemezni a fő kockázati tényezőket. Ezt a tevékenységet az iker VHF radar koncepció indítása előtt is el kell végezni, és az eredményeket a visszajelzések kapcsán, valószínűleg többször módosítani.

A közepes teljesítményű VHF radarok fejlődése töretlen a második világháború óta. A volt Szovjetunió szakemberei által kifejlesztett és Magyarországon ma is üzemelő, a magyar szakemberek által modernizált, Obarona 14 típusú radar látható az 1. ábra közepén, míg a jobb oldalon egy P-18M szintén modernizált VHF réskitöltő radar van. A 2. ábra egy amerikai a Lincoln Laboratórium által kutatási célokra épített VHF radart ábrázol. Ezen VHF radarok üzemeltetése sok tapasztalat és tudományos szempontból hasznosítható információ összegyűjtésére adott módot, melyből kiindulva az iker VHF radar koncepció sikeresen megvalósítható. A projektmenedzseléssel kapcsolatos kihívások nagyságának és az ezzel kapcsolatos kritikus pontok felmérése ennek az előtanulmánynak a fő célja.

1. ábra. Magyarországon üzemelő VHF radarok: Obarona-14 és P18-M



2. ábra. Lincoln Laboratórium VHF teszt radarja

ELŐZMÉNYEK, IGÉNYEK, LEHETŐSÉGEK

A radar rendszerek üzemeltetési és fenntartási költségei úgy hazai, mint nemzetközi viszonylatban nőnek. Ennek okai a radarok elöregedésében, az üzemeltető szakember állomány hozzáértésének csökkenésében, és a 10 vagy annál régebben beépített polcról levehető termékek és más drága alkatrészek növekvő felújítási igényében keresendő.

A légtérellenőrzés számára új feladatok és kihívások jelentkeztek, melynek megoldási lehetőségei szintén rendkívül költségesek.

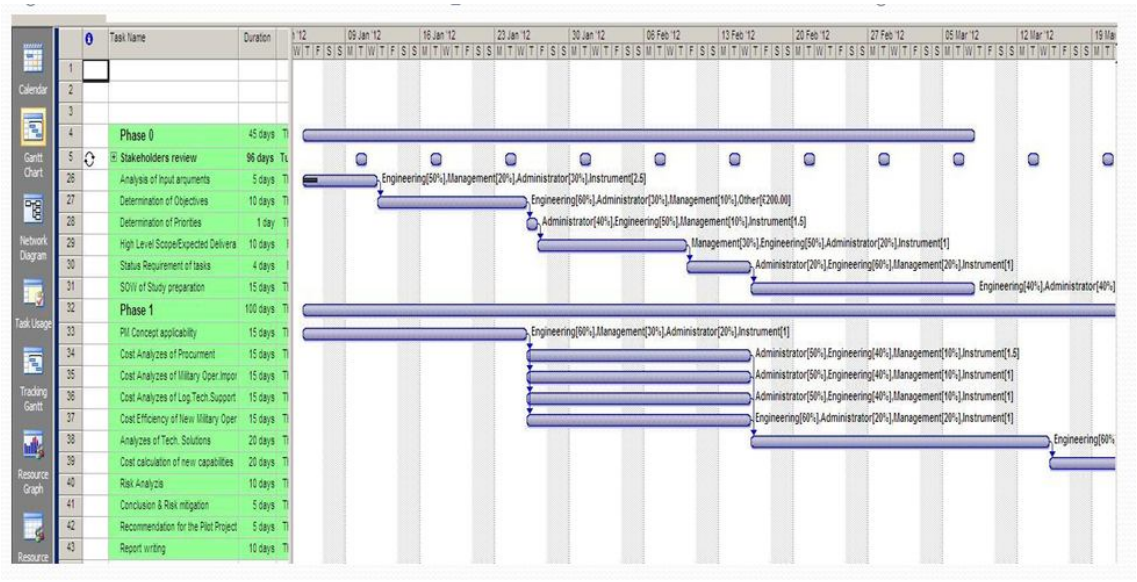
Jelenleg és valószínűleg az elkövetkező években is tart a gazdasági válság, mely rendkívül behatárolja új projektek indítását. Az előzmények kapcsolatát mutatja be a 3. ábra. Mindenesetre jogos elvárás egy megfontolt vezetéstől, hogy részletes műszaki, gazdasági és projektmenedzseléssel kapcsolatos megvalósíthatósági tanulmányok elkészítését tűzze ki célul. További elvárás lehet egy „Projekt Menedzselésen" alapuló új beszerzési, fenntartási elképzelés és munkamódszer kidolgozása és az elképzelés létjogosultságának bizonyítása egy Minta Projekt megalapozásával. A legfontosabb cél és minőségi követelmény a „MEGVALÓSITHATÓSÁG" bizonyítása. A tanulmányok legkésőbbi elkészülési határideje lehetne 2013. június 30. kb 1000 mérnökóra költségvonzataival.

A fő célkitűzések és szállítási határidők felmérése

A feladatok megfogalmazása, lebontása és GANTT Diagramban való összefoglalása napjainkban már számítástechnikai eszközökkel támogatott. Célszerűnek látszik három fázisra osztani a projektet, ahol a 0. fázis előkészítő, az 1. fázis a részletes tanulmányok elkészítése, míg a 2. fázis a minta projekt prototípusának megvalósítása. Ennek sikere esetén indulhat a sorozatgyártás.

3. ábra. Az igények egymásra hatása

Az előkészítő fázisban a feladatok lebontásra kerülnek a megvalósíthatóság, az egymásután következő eseménysorok kockázata és a megoldásra fordítható idő alapján. A tevékenységek részletes kidolgozása GANTT diagrammal átláthatóvá tehető. Ezt ábrázolja a 4. ábra.



4. ábra. Az iker VHF radar projekt GANTT diagramjának részlete

AZ ELŐTANULMÁNY LEGFONTOSABB VIZSGÁLATI TERÜLETEI

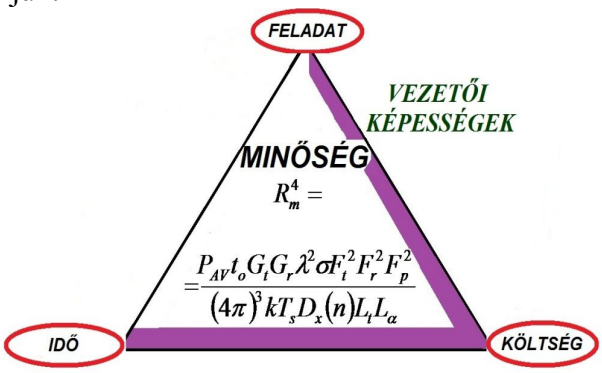
Tulajdonosi elvárások

Első lépésként a valószínű tulajdonosok lehetséges elvárásait kell felmérni. A jelenlegi gazdasági környezetben jogos igény, hogy az új légtérellenőrző radar rendszerek beszerzése és az azt követő logisztikai biztosítása költséghatékonyabb legyen a jelenleg alkalmazottaknál. További másodlagosnak tekinthető tulajdonosi érdek:

- Rövidtávon: a bevételek maximalizálása: minden elérhető erőforrásnál – ha megoldható. (Nemzetközi együttműködésekben gyakran felismerhető a clausewitzi stratégia néhány elemének alkalmazása: lásd pl. [2])
- Hosszabb távon: mértékletesség – üzleten belül maradni. Az ütköző érdekek kiegyensúlyozása.

A korszerű Projekt Menedzselés megvalósíthatósága

Minden projekt menedzsmentnek három pillére van. (Lásd 5.ábra). A FELADAT/Minőség, a rendelkezésre álló erőforrások, KÖLTSÉGEK, és a megvalósításra fordítható IDŐ. Légtérellenőrző radar rendszer esetén természetes, hogy a minőséget a radar egyenlet elvárásai alapján értékeljük.



5. ábra. A projekt menedzsmentnek három pillére

Természetesen a korszerű projekt menedzsmentnek is vannak pozitív és negatív tulajdonságai. Ennek ismerete elengedhetetlen, egyrészt, hogy ki tudjuk használni az általa nyújtott előnyöket, másrészt, hogy csökkenteni tudjuk a káros a projekt egészének sikerét veszélyeztető kockázatokat.

Az előnyös tulajdonságok:

- Jól strukturált.
- A folyamatok áttekinthetősége.
- A felelősségek pontos meghatározhatósága.
- A pénzmozgások pontos követhetősége, a Hozzáadott Érték kiszámíthatósága.
- Kockázat értékelés, és ha szükséges csökkentés.
- Minőségi munkavégzés.

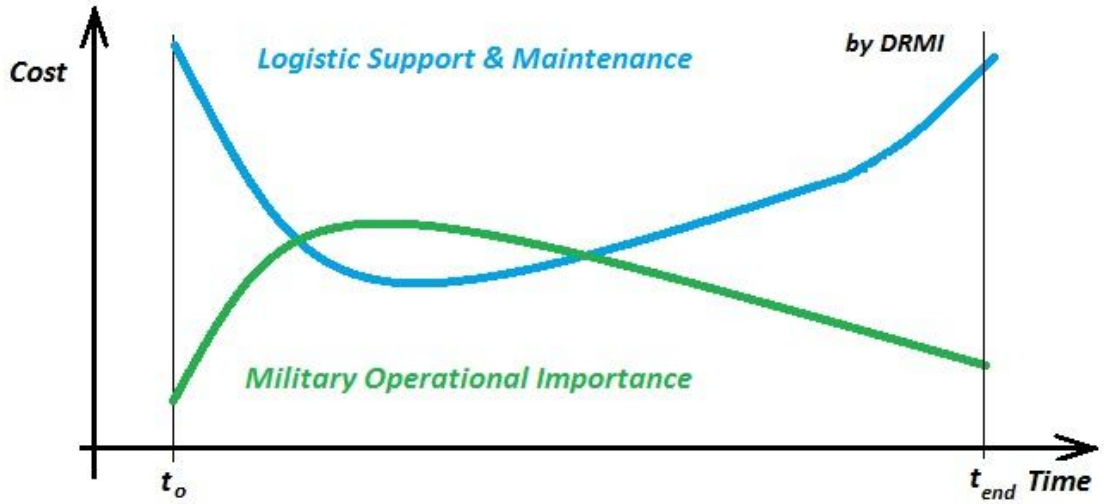
Hátrányok:

- Bevezetése költséges lehet.
- Nem alkalmazható folyamatos tevékenységekre pl. szervizelés.
- Könnyen túl menedzselhető.
- Növeli a bürokráciát.
- Egy pillér változása jelentősen növeli a projekt által felvállalható RIZIKÓT, mely ellenlépések megtételét várja el. >20% nagyobb változás csak nehezen menedzselhető még hozzáértő vezetés által is.
- Vezetés érzékeny.

Külön figyelmet kell fordítani a költségekre, hiszen a projekt résztvevők, ilyen/olyan indokokkal mind ebből szeretnének a legtöbbet „begyűjteni”. (Lásd 5. ábra költségek.) Ezért nemzetközi szinten a pénzmozgások ellenőrzésére, a projekttől elkülönülten, auditor szervezetek figyelhetik a pénzek keletkezésének és „eltűnésének” folyamatait. Különösen azok a tevékenységek veszélyesek a projekt sikere szempontjából, amikor a résztvevők közötti pénzek be- és kifizetéseit szabályozó egyenlet olyan „bonyolult” vagy „egyszerű”, hogy joggal nevezik „szépnek” vagy extrém esetekben „gyönyörűnek”. „Nice cost shearing formula”.

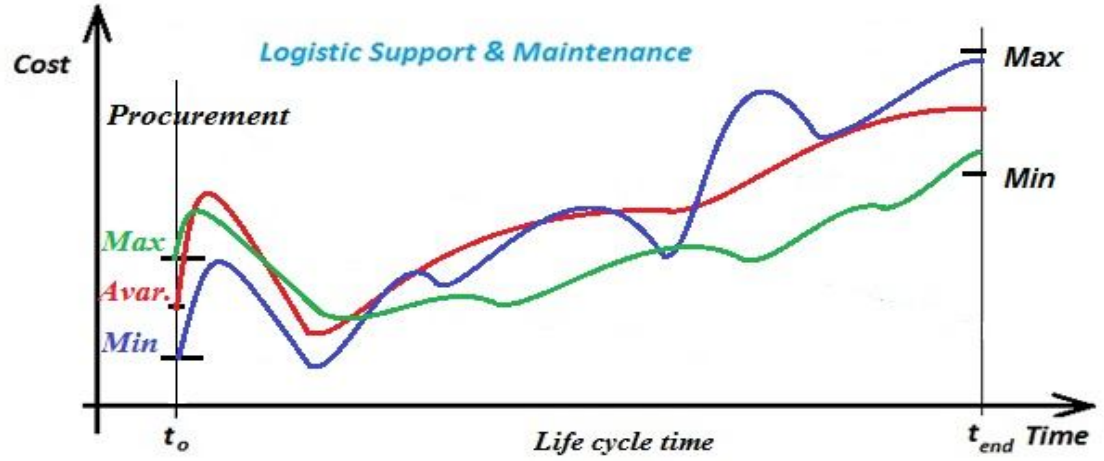
A beszerzési és logisztikai költséghatékonyság előzetes felmérése

6. ábra a költségek alakulását szemlélteti 20 éves élettartamra vonatkoztatva, a logisztikai támogatás és fenntartás, valamint a rádiólokátor vagy vezetési rendszer katonai jelentőségének alakulása függvényében. Megfigyelhető, hogy eleinte a befektetett költségek messze felette vannak az eszköz katonai jelentőségéhez viszonyítva, majd egy aránylag konszolidált szakasz következik, mely után a fenntartási költségek nőnek, de a berendezés katonai jelentősége folyamatosan csökken. Ezáltal két tényező a logisztikai költségnövekedés és a katonai használhatóság csökkenés is arra sarkall, hogy az élettartam ciklus felénél közepesen felújítsuk a berendezést. Ezáltal jelentősen csökkenthető a radar rendszer fenntartási költsége, ugyanakkor a korszerűsítés elvárásainak függvényében jelentősen növelhetjük a rendelkezésre állást és az új légvédelmi veszélyeztetettségnek való megfelelést.



6. ábra. A költségek és a katonai eszköz jelentőségének alakulása a 20 éves élettartam ciklus alatt

A 7. ábra a beszerzési ár és a 20 éves fenntartási költségek alakulását szemlélteti azokra az esetekre, amikor a radart minimális, átlagos, valamint ésszerű pénzügyi keretek közötti maximális harcászati technikai követelményekkel szerezzük be.



7. ábra. Minimális, átlagos és maximális katonai képességekkel vásárolt radarok fenntartási költségeinek alakulása a 20 éves élettartam ciklus alatt

Meglepő, hogy a beszerzési ár és a fenntartási költségek egymással fordítottan arányosak.

Statisztikai adatok bizonyítják, hogy a minimális katonai képességekkel vásárolt eszközrendszerek 20 éves élettartam fenntartási költségei 6-7 szerese a beszerzési áraknak, míg a maximális katonai elvárásokkal megrendelt eszközöké „csak” 3-3.5 szerese. Az okokat vizsgálva megállapíthatjuk, hogy a különböző helyszíni viszonyok, kezelőállomány képzettsége stb. hatnak a költségek alakulására, de ezek együttes hatása sem képes megmagyarázni a fenntartási költségekben jelentkező nagy különbségeket. Talán pontosabb magyarázatot kapunk az okokra, ha feltételezzük, hogy minden radargyártó kategóriájában a lehető legjobb radar megalkotására törekszik, hogy növelje a termék katonai jelentőségét. A gyártási és a fenntartási költségek eleve ezekre a performanciákra vannak beárazva. Ha valaki megjelenik a piacon minimális követelményekkel csak a már kész, a nagyon jó radar átszabott minimális képességekre lerontott változatát kapja. Természetesen a fenntartási költségek a nagyon jó radar performanciákra számítottak maradnak, sőt még meg is haladhatják az, hiszen az „átszabás” következtében az elvarratlan szálak kezelése új erőforrásokat követel. Valószínűsíthető az eredeti gyártó jó szakembereinek kiábrándultsága és elvándorlása új

perspektivikusabb feladatok megoldására. A profit növelését az eredeti gyártó annál is inkább megteheti, mivel nincs konkurencia a saját terméke logisztikai támogatásában.

A JELENTKEZŐ LÉGVÉDELMI VESZÉLYEK LEKÜZDÉSÉNEK MŰSZAKI LEHETŐSÉGEI

A légtérben jelentkező új légtér felügyeleti kihívások leküzdésének műszaki elemzése egy önálló megvalósíthatósági tanulmányt igényel. Ez a fejezet csak a valószínűsíthető következtetéseket tekinti át röviden.

Napjaink radar technológiája szintjén légtérellenőrzésre legelterjedtebb az „L" és „S" sávú radarok, melyek pontosak, de nem képesek hatékonyan detektálni a „lopakodó" technológiával rendelkező repülő eszközöket, időjárás, hullámterjedés és önrávezető rakéta érzékenyek. A rendelkezésre álló gyártókapacitások, szaktudás stb. miatt természetesnek vehető a továbbfejlesztésük igénye. Nagyon ígéretes megoldás a fázisvezérelt antennák általi digitális sugárnyaláb formálás technológia, mely a hadihajók és repülőgépek fedélzetén szinte egyedül alkalmazható a „több célú több feladatú" (Multi Purpose Multi Function Radar-MPMFR) radarok építésénél. Nem ennyire elterjedt, de néhány országban még fellelhető a VHF radar technológia, melyet az 1. és 2. ábrák szemléltetnek. Ezek a radarok nem olyan pontosak, mint az „L" vagy „S" sávban üzemelő társaik, de a kis radarkeresztmetszettel rendelkező célokat kb. 10-szer nagyobb visszaverő felülettel látják, sokkal kevésbe érzékenyek az időjárásra, önrávezető rakétákra és ki tudják használni a földfelszíni többszörös hullámterjedés nyújtotta lehetőségeket. Ugyanakkor az aktív „lopakodó" technológiával rendelkező repülők új kihívások elé állítják ezeket a radarokat is.

Új, a szakirodalomban még nem ismertetett radar rendszer az Iker VHF radar technológia, mely két egyforma közepes teljesítményű VHF radarból és egy jel és adat egyesítő központból áll. A két VHF radar egymáshoz néhány száz m-re települ, ezáltal ötvözi a nagy antennanyereség, adóteljesítmény többszörös energia elosztás és vétel nyújtotta előnyöket. harcászati-műszaki követelményeit tekintve egyedülálló képességekkel rendelkezik.

Nagyon fontos megemlíteni a különböző passzív radar rendszereket, melyek képesek rádió, TV, GSM hálózatok adójeleit felhasználni egy kiterjedt Hálózat Centrikus rendszerben. Ide tartozhatnak a korszerű infra- és optikai berendezések is. Sőt, Napunk, mint univerzális nagyteljesítményű adó szinte minden hullámtartományban használható a passzív radar rendszerek számára.

A műszaki lehetőségek pénzügyi vonzatai

Értékbecslés szempontjából pontosabb eredményt kapunk, ha a perspektivikus radar rendszerek összehasonlítására szolgáló költségeket – a beszerzési ár és a 20 éves fenntartási költségek összegeként képezzük. Viszonyítási referencia árnak tekintsük a legújabb *L/S sávú radar technológia* így képzett költségét és jelöljük - $Y_{átlag}$ árnak. A „több célú több feladatú" *MPMFR technológia* a kis területre sok képesség összezsúfolása elv miatt ötszöröse a legújabb L/S sávú radar technológia árának - $5 \times Y_{átlag}$. Ezekhez képest az 1. és 2. ábrán látható *VHF radar technológia* csak - *0.2 x Yátlag.*

Az *Iker VHF radar technológia* ára a komplexitás miatt - *3x 0.2 x Yátlag*, míg a *passzív* felmerülő *radar technológiák* rendkívül *olcsón megvalósíthatók***,** amíg a civil és a katonai alkalmazás közel van egymáshoz. A hiányzó katonai képességeket költséges kiegészítő fejlesztésekkel kell biztosítani. Ugyanakkor ezek a megoldások könnyen integrálhatók minden fent megnevezett radar projektbe, mint azok alrendszerei.

A projekt szempontjából fontos további elvárások

A VHF frekvencia rádiólokációs célokra való európai alkalmazása nincs megoldva. Az ezt a frekvenciasávot alkalmazó országoknak hivatalosan kell kérni a VHF frekvenciatartomány rádiólokációs célokra való alkalmazását. Ugyanakkor lehetséges a nagyon nehezen kimutatható LPI (Low Probability of Intercept – Kis valószínűséggel észlelhető) radar technológia fejlesztése és alkalmazása. Ezek a radarok széles spektrumú, zajszerű adójeleket használnak eltűnve a környezeti interferencia hátterében.

Új feladatként jelentkezik a projekt három alappillérének a prototípusra és gyártásra vonatkozó elvárásainak meghatározása. Nagy valószínűséggel prognosztizálható, hogy az erőforrások és a határidőkre vonatkozó elvárások optimalizálhatóak, míg a célok és minőségi követelmények alapvetően nem változhatnak. A 20 évre tervezet logisztika főbb kérdésköreit az 1.táblázat foglalja össze. Itt a logisztikai támogatás három nagy csoportba sorolható. Ezek:

- Hagyományos logisztika – ahol a katonai szervek és/vagy a gyártól független nem profit orientált szervezet felelős és végzi a rendszerek üzemeltetéséhez szükséges tevékenységet. Az eredeti gyártó szolgáltatásait csak rendkívüli esetekben veszik igénybe. Napjainkban ez a módszer a legelterjedtebb a világon.
- CLS – ahol az eredeti gyártó, a gyártmány élettartamára teljes körű logisztikai szolgáltatást biztosít. A katonai szervek csak az „átvételek" igazolásáért felelősek. Gyakran igénybe veszik az eredeti gyártóktól független SPC szolgáltatásokat a radar valódi „In Situ" performancia felmérésére. Kísérleti jelleggel már több rendszert ilyen módon üzemeltetnek a világban.
- Kevert szolgáltatási struktúra – mely ötvözi az első és a második módszert. A Hagyományos logisztika hiányosságai jól ismertek a szakemberek között, bár legnagyobb előnye a harcszerű körülmények közötti hadrafoghatóság magas szinten tartása vitathatatlan. A CLS koncepció, maga is egy projekt, mely jelentős kockázatot rejt magában elsősorban profitorientáltsága miatt, lásd 5. ábra, másodsorban a gazdasági környezet változása miatt, ahol a csődök, akár országos szinten is jogutód nélkül felszámolhatja az ORM-t. Ezen érvek alapján a kevert szolgáltatási struktúra kialakulása egy természetes folyamat végterméke, ahol a logisztikai feladatokat felosztják egymás között a projektben részt vevő katonai és ORM-t képviselő felek. Ezen a területen a legkritikusabb láncszem a Demarkációs interfészek (HW, SW) és jogi felelősségek szerződésben való rögzítése.

A jelölések magyarázata: CLS – Contractor Logistic Support (az eredeti gyártó által a gyártmány élettartamára biztosított teljes körű logisztika), ORM – Original Radar Manufacturer (A radar eredeti gyártója), HMK – Harcászati Műszaki Követelmények, SPC – System Performance Check (Rendszer performancia ellenőrzés, „In Situ"), PDS – Post Design Service (Újítások és modernizálások)

Terminológia		A logisztikai támogatás típusa		
		Hagyományos	CLS	Kevert
Elgondolás	Kezdet	Szerviz (Katonai), Vizsgálatok (SPC) (Katonai) Modernizáció (PDF) (Katonai)	Szerviz (ORM) SPC (Katonai) PDS (ORM)	Szerviz (ORM) SPC (Katonai) PDS (ORM, Katonai)
Értelmezés	Tervez	Erőforrás tervezés, Kidolgozás, Szállítások,	Kick-off; Részletes HMK; SPC tervezés & előkészítés (Kat.)	Kick-off; Részletes HMK; Demarkációs interfészek (HW, SW) és jogi felelősségek; SPC tervezés & előkészítés (Kat.)

Végrehaj -tás	Végre-hajt	Építkezés/telepítés SPC/PDS Végrehajtás	Építkezés/telepítés SPC/PDS (Kat.) Végrehajtás (ORM)	Építkezés/telepítés (ORM) SPC/PDS Végrehajtás (Kat./ORM)
Befeje-zés	Lezár	Szállítások, Átvételek és Fizetési határidők	Szállítások, Átvételek és Fizetési határidők	Szállítások, Átvételek és Fizetési határidők

1. táblázat.

A KOCKÁZATOK ELEMZÉSE

A projekt koncepció nagy előnye, hogy általa nagy valószínűséggel feltárhatók a projekt fő kockázati tényezői. Ezért vizsgáljuk meg, hogy milyen kockázatokat rejt magában, ha az új katonai elvárásokat hagyományos beszerzési és logisztikai biztosítással valósítjuk meg. A 2. táblázatban összefoglaltam a szerintem legfontosabb kockázati tényezők eloszlását. (Az elemzés segítésére több jól működő számítástechnikai SW csomag letölthető az Internetről, melyek alkalmazásával nagy valószínűséggel felmérhető a projektek kockázata. Az előtanulmány számára elégséges pontosságot szolgáltatnak a legegyszerűbb szoftverek is.) A 2. táblázat vízszintes sorai az adott tevékenység kockázatát jelzi „Alacsony”, „Közepes” és „Magas” értékeléssel, míg a függőleges sorai a kockázat hatását „Alacsony”, „Közepes” és „Magas” besorolással.

Hatás *Kockázat*	Alacsony	Közepes	Magas
Alacsony	Megvalósíthatósági tanulmány	Fejlesztés	Infrastruktúra
Közepes	Elemzések HMK	Kivitelezés, Telepítés	Túlköltekezés
Magas	Határidők	Prototípus	PM ;Logisztikai támogatás

2. táblázat. Kockázatok a hagyományos módszerek alkalmazásával

A 2. táblázatból látható, hogy legnagyobb kockázatot a Projekt Menedzsment és a Logisztikai támogatás jelenti. Mindkettő kockázata csökkenthető a kiképzés gyakoriságának és minőségének emelésével. A prototípus legyártásának kockázata magas, mivel a szerződés aláírása után a gyártó egyedül van a piacon, ráadásul nagyon profit orientált. A megrendelő részéről a projekt előrehaladásával szintén egyre nehezebb a kudarc beismerése, mivel nehéz alternatív megoldásokat találni, így természetes, hogy az 5. ábra valamennyi pillére változik. A túlköltekezés természetes következménye ennek a struktúrának, különösen, ha a gyártó az egyedüli, aki a radar élettartama alatt a logisztikai feladatok ellátásáért felelős.

Ezeket *a kockázatokat csökkenteni kell,* mely megoldható a beszerzési eljárás és a logisztikai támogatás módszereinek korszerűsítésével. A beszerzési eljárás korszerűsítésének irányához ad némi alapot a 7. ábra és az 1. táblázat kapcsán felmerült lehetőségek további vizsgálata. Ezek alapján valószínűsíthető, hogy célszerű áttérni a Minimális Katonai Követelmények eljárásról a Maximalizált Költséghatékonyan Elvárható Katonai Követelmények eljárásra. Ennek lényege a Nobel díjas közgazdászok által bizonyított tenderezési eljárás, ahol a tender kiírásra jelentkező cégek közül a legdrágább és a legolcsóbb ajánlat automatikusan kizárásra kerül és a bennmaradók közül az összességében a legjobb műszaki paraméterekkel rendelkező cég nyeri el a projektet a szállítások 2/3-ra. A második helyezett szintén jogot kap a prototípus elkészítésére és a szállítások 1/3-ra. A legjobb katonai műszaki paramétereket a prototípusokon elvégzett ellenőrző vizsgálatok döntik el. Ezáltal

biztosítható a cégek között bizonyos fokú verseny és a felhasználók kiszolgáltatottsága csökken, a mérnök műszaki állomány megbecsülése növekszik. Ezek után természetes, hogy a berendezések logisztikai támogatásánál legalább ennek a két cégnek a versenyeztetési lehetőségét fenn kell tartani. Ezért és a harctéri üzemeltetés flexibilitásának növelésére a katonai rendszereket nemcsak moduláris egységekből kell felépíteni de, a felhasználó által meghatározott modul egységek interfészeket egymással csereszabatosan kell leszállítani.

A lehetséges költségcsökkentő módszerek további elemzésekkel tovább finomíthatók, de már ezen eredmények alapján érdemes a mintaprojektet az új elvárások szerinti kockázatelemzéssel megvizsgálni. Ezt elvégezve és a 2. táblázat értékelési szempontjai alapján a 3. táblázat szerint valószínűsíthetők a mintaprojekt kockázatai.

Hatás *Kockázat*	Alacsony	Közepes	Magas
Alacsony	Megvalósíthatósági tanulmány, Elemzések	Túlköltekezés, Kivitelezés	Infrastruktúra
Közepes	Határidők, HMK	Prototípus, Telepítés	PM
Magas	Fejlesztés	Logisztikai támogatás	A koncepció elfogadtatása

3. táblázat. Kockázatok az új módszerek alkalmazásával

A legfontosabb következtetések az új koncepcióval kapcsolatban:

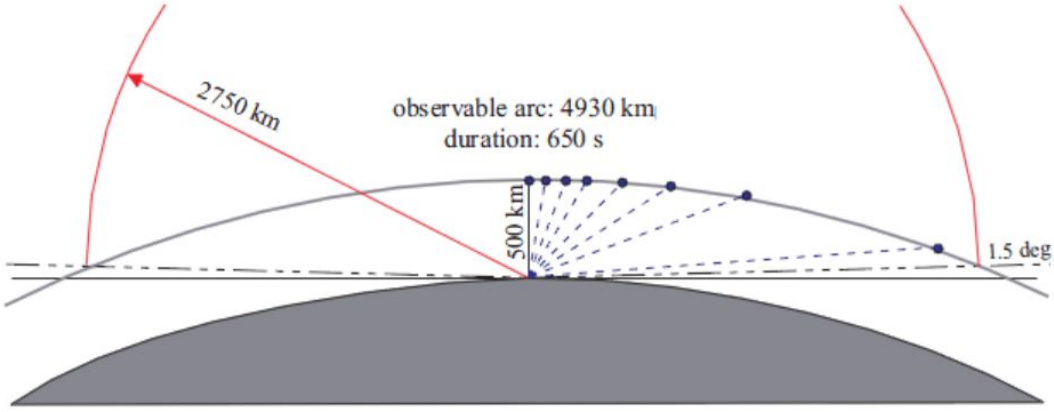
- A kockázatok jelentősen csökkennek.
- A megvalósítás költségei csökkennek.
- A vállalt határidők tartásának valószínűsége jelentősen megnő.

Ugyanakkor az új projektmenedzselés sem teljesen kockázatmentes. A mintaprojektnek a legnagyobb problémája és a vezetés megoldandó feladata a „A koncepció elfogadtatása”. További kihívást jelent a Projekt Menedzselés munkája és az új elvárásoknak megfelelő munkamódszerek kidolgozása és elfogadtatása. A logisztikai támogatás azért kapott előkelő helyezést a kockázatok sorában, mivel hosszú időtartama miatt a gazdasági környezet és a műszaki lehetőségek jelentősen változni fognak.

A fentiek alapján nagy valószínűséggel megállapítható, hogy az iker VHF radar technológia a legköltséghatékonyabb és a legkevésbé kockázatos megoldást kínálja korunk légtér-ellenőrzési kihívásainak megoldására és a mintaprojekt indításához.

Lehetséges kapcsolat más projektekhez

Nem túljelentős, de az európai országokkal összehangolt tevékenységet kíván a VHF frekvencia rádiólokációs célokra való európai alkalmazásának engedélyeztetése. Ebben a folyamatban valószínűleg segítségünkre lehet az a tény, hogy az EU is felismerte az „European Space Situation Awareness System” kialakításának szükségességét. 2009 januárjától feladata megvalósíthatósági tanulmányok kidolgozása az Európa feletti alacsony pályán, 80 és 500 km-s magasság tartományban, keringő műholdak és egyéb objektumok detektálására, útvonalba fogására és azonosítására. A 8. ábra a földi telepítésű radar rendszer feladatainak nagyságára mutat rá.



8. ábra. A földi telepítésű radar űrmegfigyelési paraméter elvárásai

A radarnak a horizont felett másfél fokkal kell detektálási képességekkel rendelkeznie a földfelszíntől számított maximum 500 km magasan keringő műholdak detektálására. Így a megfigyelt útvonal nagysága majdnem 5000 km és ezen a magasságon az egyenletes sebességgel „zuhanó" műhold 650 másodpercig tartózkodik a radar felderítési zónájában.

Erre a feladatra már működik Európában az orosz űrmegfigyelési hálózat a VHF frekvencia tartományban, és a hasonló feladatok ellátására tervezett európai radar hálózat számára is fontos a VHF frekvenciatartomány. Ugyanakkor a VHF frekvencia tartomány, a szűkös sávszélesség miatt, egyre értéktelenebb a civil felhasználók számára. Ezért minden lehetőség adott az frekvenciasáv radar célokra való engedélyezésére, különösen, ha az iker VHF radar koncepció műszaki lehetőségei következtében helyet kap ebben a programban és a rendszer legalább egy eleme Magyarország sík területén kerül telepítésre.

Fejlesztési határidők

Ezek alapján érdemes felmérni az iker VHF radar rendszer prototípusának és gyártására vonatkozó várható határidők alakulását a főbb elvégzendő feladatok függvényében. Ezt a 4. táblázat tartalmazza.

Követelmények a Prototípusra	Idő	Követelmények a Gyártásra	Gyártási idő (a Prototípus után)
Kick-off (Indítás); HMK	1 év	Kick-off; HMK pontosítás	0.5 év
HW & SW beszerzés/ fejlesztés	3év	HW & gyártmány	2 év
HW & SW tesztelés/ hangolás	2 év	Tesztelés, Installálás	0.5 év
Test eredmények elemzése, Záró jelentés	0.5 év	Kiképzés, Átvételek	0.5 év
Kevert Verziós Logisztika	20 év	Követelmények	3 év próbaidő

4. táblázat. A Prototípus és a Gyártmány időszámvetése

Megállapítható, hogy a prototípus 3 év alatt legyártható és 2.5 év szükséges a részletes tesztek elvégzéséhez és az eredmények kiértékeléséhez. A projekt indítása után számított 7. évben indulhat a 20 éves logisztika, egy 3 éves nagy figyelmet igénylő próbaidős szakszolgálattal (ha a prototípusok alkalmasak a katonai üzemeltetésre). Eredményes prototípus után a 7. évben indulhat a sorozatgyártás, ahol a gyártási és üzembe állítási idő kb. 3 év.

VÉGSŐ KÖVETKEZTETÉSEK, JAVASLATOK

Az új beszerzési és logisztikai támogatás rendszere érdemes a figyelemre, mivel költséghatékonyabb és kockázatmentesebb a jelenleg alkalmazott megoldásoknál. Ezért érdemes további erőfeszítéseket hozni a mintaprojekt indítására való felkészülésre.

Az iker VHF radar rendszer bizonyíthatóan perspektivikus és költséghatékony alternatíva minden más megoldással szemben, ezért a részletes megvalósíthatósági tanulmányok elindítását mielőbb meg kell kezdeni. A fejlesztéseket frekvencia engedélyek nélkül is érdemes elkezdeni a Kis valószínűséggel észlelhető (LPI) technológia alkalmazásával.

Felhasznált irodalom

[1] A Guide to the Project Management Body of Knowledge (PMBoK^{TM}), 4th Edition, Project Management Institute, 2008

[2] Clausewitz Károly, A háborúról, 47.oldal, Göttinger kiadó, Veszprém, 1999.

[3] Dr. V. Chernak : Fundamentals of Multisite Radar systems, Gordon & Breach Science Publisher, 1998; ISBN-10: 9056991655 ;

[4] D.K.Barton: Modern Radar System Analysis ver. 3.0 Software and User`s Manual, Artech House, Inc. 2007. ISBN 13:978-1-59693-264-7

[5] Zsolt Haig: Connections between cyber warfare and information operations, Vol. 8, No. 2 (2009) 329–337, ISSN 1788-0017

[6] Stefan Ban: Next Generation Multi Functional Surveillance and Target Acquisition Radars Using New Technologies, IRS 2011, Proceedings p.27-29.

[7] Joachim Ender, Ludger Leushacke, Andreas Brenner, Helmut Wilden : Radar techniques for space situational awareness, IRS 2011, Proceedings, p.21-26.

[8] Marc Lesturgie: Some relevant applications of MIMO to radar, IRS 2011, Proceedings, p.714-721

[9] K. E. Olsen, K. Woodbridge, ”Performance of a Multiband Passive Bistatic Radar Processing ‚Part II”, IEEE AES System Magazine (AESSM) Special Issue on Passive Coherent Location, invited paper submitted 31. August 2011.

[10] Ványa László: Az INTERJAM projekt első éve, Robothadviselés 8. tudományos konferencia Budapest, 2009

[11] Kende György: A sakk, mint hadijáték és a képességfejlesztés eszköze, Hadtudomány, 2006. 1-2. szám, ISSN 1215-4121, pp. 101-110

[12] Kunos Bálint: A haderőreform haditechnikai aspektusai, HADTUDOMÁNY X. évfolyam, 3. szám, http://www.zmne.hu/kulso/mhtt/hadtudomany/2000/3_3.html

[13] Kovács László, Illési Zsolt, Cyberhadviselés: Hadtudomány, MHTT Konferencia, http://mhtt.eu/hadtudomany/HT-2011_1-2_5.pdf

[14] Végh Ferenc: A Friedman-elmélet I./II. Haditechnika, 2011, 3. szám 13-17 oldal, 4. szám 9-12 oldal

[15] Bálint Kunos: Defence economy and the European Union. Tradecaft Rreview (Special Issue), Budapest, Hungary 2010

[16] Balajti István: Az iker VHF radar stratégiai jelentősége a modern légvédelemben, Robothadviselés, Tudományos konferencia, 2011, November 24, Budapest

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Inkovics Ferenc
ferenc.inkovics@gmail.com

SECURITY TECHNOLOGY AT MISSIONS OF HUNGARY

Absztrakt/Abstract

Az elmúlt évtizedekben a biztonság központi kérdéssé vált a világban. A biztonságtechnikai eszközök a mindennapi életünk részei lettek. A magyar diplomáciai és konzuli szolgálat Magyarország legtávolabbi védővonala, ezért a biztonság nagyon fontos a magyar külképviseleteknek. E cikk bemutat néhányat a vagyonvédelmi felszerelésekből, lehetőségekből és a Külügyminisztériumban alkalmazott megoldásokból.

Security has become a central problem in the course of the past decades. The means of security technology have become a part of our everyday life. The Hungarian diplomatic and consular service is the farthest defense line of Hungary, and security is very important for the Hungarian missions. This article reviews first of all property protection equipment and possibilities of security technology, furthermore the methods applied by the Ministry of Foreign Affairs of Hungary (MFA).

Kulcsszavak/keywords: *biztonságtechnika, informatika, külügyminisztérium, külképviselet ~ security technology, IT, information technology, Ministry of Foreign Affairs, mission, representation*

INTRODUCTION

A great number of circumstances endanger the life of people and many of them erroneously regard security as a means or a system of means although security is a status. Exactly this is the lack of being endangered and, of course, everybody would like to live in security. The status of being threatened cannot be completely eliminated but the risk of its occurrence can be minimized. For this applying the solutions of security technology can be the proper means. But what is security technology?

According to the university notes "The bases of Security Technology" [1]: the concept of security technology is the territory of technical sciences where the task is given to increase the security of different objects and systems to diminish the risk of property damages and the harmful effects hitting people by applying technical, organizational, health and economic means and measures.

This is the reason why we nowadays so often meet the expression "security technology" in a very wide circle e.g. in case of cars, working places, apartments, airports and even in the case of IT. In the course of our everyday life we also meet means and solutions of security technology when we enter a bank, are walking in the streets or when we depart from an airport for a long weekend. This article reviews first of all property protection equipment and possibilities of security technology, furthermore the methods applied by the Ministry of Foreign Affairs of Hungary (MFA).

PROPERTY PROTECTION

In life, we often meet simple and complex security problems and questions. However, the solution of complex questions consists of smaller and simpler steps. One of the best security experts of the world, Mr Bruce Schneider1, elaborated a method consisting of five simple questions how to put the security problems of governments, companies or individuals into a coherent unit that can be more easily handled. Proper consequences and compromises can be deducted from this coherence. [2]. The questions are as follows:

- What are you trying to protect?
- What are the risks to those assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

If a complex security problem is divided into smaller steps, that does not mean that a complex solution is not necessary. These property protection solutions may consist of mechanical protection, manned guarding and security, personal protection, as well as electronic protection or some kind of combination of all these. Here below we can see the details of complex property protection and its elements:

- Mechanical protection
  - Outdoor property protection solutions (trenches, embankments, fences, gates, crossing gates, etc.)
  - Construction and entering points of buildings (shell elements, walls, flooring, platform/bridging/, bars, shutters, doors, windows, locks, padlocks and iron mountings, etc.)

1 At present Bruce Schneier is the BT (British Telecom) Security Chief and he also issues monthly a free newsletter on security.

    - Security storage for valuables (fire proof lockers, strong-boxes, strong-rooms, safes etc.)
    - Mechanical protection of persons (bullet-proof vests, body armors, etc.)
- Manned guarding and security
    - Key Point protection[2]
    - Territory protection
    - Combined protection
    - Patrolling
    - Protection of persons
    - Guarding of sport events and mass movements (demonstrations, performances, etc.)
- Electronic protection
    - Fire alarm and fire fighting techniques
    - Burglar alarm
    - Industrial video systems (formerly CCTV systems)
    - Inspection/controlling systems and equipment of persons and baggages
    - Goods protection equipment
    - Positioning systems
    - Remote control and transmission systems.
    - Access control and working-ours recording systems.
    - Buzzer and door phone systems

When checking thoroughly the above, we can see that an increasing number of integrated ICT means can be found in the solution of security technology. Formerly instruments of security technology, also used low voltage solutions, but nowadays the proportions are shifting towards ICT solutions. Electronic solutions can be found in an increasing number in devices. E.g. when passing through the rooms of a building it can be seen that practically most places require the installations of fire alarm, electronic means that can be connected to the computer network system (computer workstation, telephone, network printer, multifunctional copier, etc.) and some kind of property protection device (e.g. sensors for doors and windows and movement sensors, readers for entering systems, etc.) Therefore if an older building is going to be renovated, modernized or a new building is constructed, nowadays it is advisable to fix and to execute the endpoints and cables of property protection, fire protection and ICT systems simultaneously during the projecting and construction period. It is possible that complex projecting and execution will involve somewhat higher costs, nevertheless, this requires lower costs than a posterior solution or modification, not to mention esthetic and functional compromises.

Most companies and organizations dealing with this subject handle these methods and solutions as a complex unit. It cannot be assumed that a fire protection expert, property protection expert or ICT expert is equally familiar with all three questions. Each field of activity has its own experts.

As it can be seen from the above, the modern or up-to-date fire alarm or property protection systems contain more and more ICT novelties. Today, thanks to the above, not only the security cases (e.g. alarm in case of fire or illegal entering) can be transferred to great distances, but due to the up-to-date technical devices we can get a full picture of the happenings at the site or probably even can influence the actual local proceedings. An increasing number of solutions based on IP (Internet Protocol) can be found (e.g. wireless

2 Key Point Protection is a kind of property protection and means protecting the key important place or area of the object that is essential in terms of being endangered e.g. an entrance, a place – cashier's office, telephone center) etc.

camera systems, where each camera has its own IP address and through the computer system the visible data can be recorded and/or observed at the actual time at the site).

SECURITY TECHNOLOGY AND THE HUNGARIAN MINISTRY OF FOREIGN AFFAIRS

The Hungarian diplomatic and consular service is the farthest defense line of Hungary, assists in signaling unwanted threats (terrorism, organized crime, epidemics, and illegal migration) detects the unwanted persons by checking their authorization to enter. In connection with trips it renders help3 to passengers traveling to catastrophe-hit and crisis areas as well as to citizens abroad in trouble. Therefore when we travel abroad it is important to take with us the address and phone number - and any other contact information - of the respective Hungarian consulate(s).

Since 11 September 2011 the danger of terrorism has significantly increased all over the world. The Hungarian missions are also affected by this fact, however, they have not become a direct target of terrorist attacks. Security has nevertheless become a central problem in the course of the past decade. It is the receiving country's task to guarantee the security of Hungary's diplomatic mission and representatives. Reasons:

Articles 22 and 29 of the Vienna Convention of 1961 (Vienna Convention on Diplomatic Relations) [3] defines the immunity of the premises of diplomatic missions and the personal immunity of the diplomatic representatives. This agreement includes that the receiving country is obliged to protect with proper measures the premises of the diplomatic mission against any intrusion damages, and hinder and stop the possible disturbance of the diplomatic mission and hurting its dignity. Furthermore, the receiving country is obliged to take proper measures to inhibit actions against the liberty and dignity of the diplomatic representatives. The receiving country is obliged to honor the inviolability of the buildings of the diplomatic mission even in case of an armed conflict, even in case the diplomatic connections had been severed or the diplomatic representatives had already - temporarily or finally - returned to their home country.

According to the above, in order to guarantee the security of the sending country's premises and representatives and if the international situation requires police officers shall be posted in front of the diplomatic missions in Hungary, e.g. to strengthen the police protection of the US Embassy following the death of Bin Laden [4]. There are, of course, cases when police presence in front of a diplomatic mission at the request of the diplomatic representative is required. In such cases - of course - against payment is effected by the sending country. There were cases in the past when the mission of Hungary has requested police protection for the Hungarian mission in certain states.

Every country may choose its own method how to meet its protection obligations. International law requires not only the protection and immunity of the representation and its members but identical rights are granted for the head of mission's premises, i.e his residence, and the home of diplomatic representatives, as well. In Hungary the procedure concerning the protection of diplomatic missions is regulated by a governmental edict. According to this the national security services, the Ministry of Interior and the Protocol Department of the MFA together classify the protection level of the threats into 3 categories. During this categorization the possible request of the representation in question, respectively the non-

3 This expression is often misunderstood by many citizens. E.g when spending our holidays abroad, our valuables are stolen or we suffer an attack we can contact our consulate for help in searching a reliable legal adviser but this will not be supplied at the expenses of the consulate. When travel documents are stolen these will be replaced by the consulates but at the travelers' expenses.

public information available through international connections will be taken into consideration. In addition to the 1961 Vienna Convention (this international treaty defines a framework of diplomatic relations between independent countries) there are independent international conventions/treaties regulating the necessary requirements for the protection and immunity of the international organizations and their members.

It is necessary to mention the 1979 "New York Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents". This itemizes what steps must be taken and what co-operation must be carried out in case of organized or committed attacks against heads of states and governments, government members, special delegations and diplomatic representatives, respectively it regulates the prevention methods, as well.

According to the level of security endangerment, the missions can be categorized. Most representations belong into the first category. These can be found in states that can meet their obligations according to the Vienna Convention. Representations of the second category can be found in states where a legitimate police power exists but public safety is on a poor level and the receiving country is not fully capable to guarantee the security. In the third category there is a legitimate police power but as far as internal politics is concerned it is rather unstable. In case of the fourth category there is no legitimate police power available, therefore the receiving country is not in a position to meet the requirements of the Vienna Convention.

For most Hungarian diplomatic missions the receiving country can secure a proper level of security, although cases may occur where the receiving country cannot meet the requirements of the Vienna Convention. Only in cases of diplomatic missions belonging into the third and fourth category may exist the necessity that the sending state should solve the guarding and protection of the diplomatic mission. At present, Hungary has no diplomatic mission where such protective measures would be necessary, but the Hungarian diplomatic mission in Baghdad was in such a situation in 2004. Due to economic, political and diplomatic reasons or eventually obligations accepted in international treaties Hungary may have to ensure the protection of its own diplomatic mission and representatives. However, the question may arise: who will perform the protection of the Hungarian diplomatic missions, in case the receiving state cannot meet its obligations required by the Vienna Convention. Three possibilities may arise:

- Hungarian Defence Forces: On international level one can see similar actions of the United States, according to which diplomatic missions of the USA are protected by marines. E.g. Israeli embassies are protected by Israeli servicemen, however, it must be remarked that they have the right to carry fire arms but these can only be used on the territory/premises of the representation! The question may arise: why don't Hungarian soldiers protect the Hungarian representations. Hungarian law does explicitly give no authorization for that. But according to the decision of the Hungarian Parliament the Hungarian Defence Forces participated in the Iraqi International Forces. The Hungarian diplomatic service carried out the receiving and forwarding of "military mail" between Hungary and Hungarian mission in Iraq with the participation of Hungarian Defence Forces. For this purpose Hungarian soldiers were sent to the Baghdad Embassy of Hungary from the authorized military contingent. Naturally, these soldiers together with the Hungarian diplomatic representatives participated in the security protection of the Embassy. Hungarian Defence Forces have to protect establishments that are of prime strategical importance to the military protection of the Republic of Hungary. The Hungarian diplomatic missions are not such establishments therefore the protection of the diplomatic missions does not belong to the protection activities of the Hungarian Defence Forces.

Possible changes of the respective law may come into effect in the future and can make way for this possibility to come true.

- Police force: reverting to the cooperation figuring in point 1 the Hungarian Government decided in 2004 that the protection of diplomatic representation had to be secured by Hungarian policemen [5]. Furthermore, the government authorize the minister of internal affairs to establish a quick-action guard unit with 50 members that can guarantee the security of the Hungarian diplomatic missions stationed in crisis areas [6]. However, this unit had not been put in action therefore it is the Hungarian MFA that exclusively secures the protection of the Hungarian diplomatic missions at present.
- Personal and property protection firms: no such firms have been put in action in Hungary. Should the necessity arise, then it must be taken into consideration that such firms have no licenses issued by the authorities neither in Hungary nor in a foreign state therefore these cannot take forceful measures and exercise authorized power. As they are not in possession of licenses issued by the authorities in case of their employment the receiving country will not grant them any immunity and help.

As already mentioned above, most states are able to meet Vienna Convention obligations. Despite this, it is necessary to undertake steps for preventive and protective measures characteristic for the site, or respectively defined in their own security regulations, as exercised by the citizens, organizations and enterprises of the given country.

It is a well-known fact that in Hungary more and more buildings, residences and facilities are supplied with security cameras, alarm systems, different property protection installations, even with watchdogs and manned guarding. The same can be observed at MFA's buildings in Hungary and in its missions all over the world, too. However, there are differences between a residence, a shopping center and MFA buildings. E.g. high ranking representatives of different foreign states or even heads of states are often visiting the premises of MFA and diplomatic missions, where classified and electronic documents are also handled, prepared, stored and forwarded, therefore strict security instructions and measures must be applied for their security and protection.

Handling of classified data, that can be of Hungarian or foreign origin (NATO, EU, WEU etc.), must correspond to special security regulations. The legal regulations concerning the handling of classified data define personnel, physical and administrative security requirements and measures. This article deals with only physical security. Instruments and methods of security technology have to be applied for evolving physical security. Physical security has internal intermediate and external elements. The external elements are used for protection of territorial outer limits. The intermediate elements signal the unauthorized entrance to the manpower or response forces. The internal elements delay or even inhibit the obtention of classified material by unauthorized persons. In order to protect classified materials, therefore these can only be handled, prepared and stored at a properly secured area corresponding to the required classified level, therefore three different areas are required for classified material handling [7]:

- administrative zone: every area where entrance is controlled
- second class security area: every site where “Confidential” or even materials of higher classification are used, or used and stored, or just stored in a way that unauthorized access can be inhibited by internal measures. The area is physically separated and protected, furthermore the entrance and departure is controlled. In order to hinder the unauthorized access to classified data, to enter this classified area is made possible only by special authorization. Persons without a personal security certificate can only enter when accompanied by an escort.

- First class security area: every site where “Confidential” or higher classified materials are handled, or handled and stored, or stored in a way that the entrance to the area means access to the classified material, as well. The area is physically separated and protected as well as entrance and departure are controlled. Entrance and departure are possible only through an access control system and only for those who possess a special authorization and a personal security certificate.

To establish a security zone at a diplomatic mission depends on various circumstances. Local characteristics, such as the building of the mission rented or owned, situated in an individual or office building, strongly influence the cost of security zone installations. Security instructions and requirements must be observed, not only at home but everywhere in the world, independent of the fact whether the mission is operating on the territory of a friendly state (EU/NATO) or in a country threatened by international terrorism.

As it is necessary to protect the security interest of the Hungarian state execution, modification and maintenance of the system can only be carried out by technical personnel sent by Hungary. First class security areas are the most expensive ones to establish and maintain. These will be executed at larger representations being of prime importance from the viewpoint of strategical, economic, diplomatic, political relationship and concerning the foreign policy of the Hungarian government. It is a well-known fact that such security areas can be found not only at diplomatic missions of Hungary but practically at diplomatic missions of every state. The protection of security zones involves special human and technical requirements. The entrance into such a security zone is strictly limited and only permitted for few who have authorized access to these data. The entrance regulations have to be applied under strictly controlled conditions and the entrance itself (persons, duration etc.) must be continuously registered. Before beginning to handle classified data, it is necessary to elaborate the personnel, physical and administrative security conditions and the personnel must be subjected to a proper security check. They are obliged to pass an examination proving their knowledge of the regulations, and their observing of these regulations must also be checked continuously. Only full knowledge is accepted.

At certain strategically important mission so-called security expert services (KBSZCS – standing for “Külügyi Biztonsági Szakértői csoport” - a Hungarian abbreviation of Expert Group for Security of Foreign Affairs) must be formed and maintained [8]. In every case this means a 7/24 hour duty on security services continuously, i.e a continuous every day service of the week. At missions with such services the duty personnel renders the first line of manned response.

On higher level security areas, protection against technical attacks must also be established or introduced. The purpose is to aggravate access to information of great importance for us. Therefore the following details are also of great importance: wall thickness, quality of the bars, brake-through time factor of the doors, existence of security illumination and cameras (CCTV – Closed Circuit Television), their installation points and viewing angles, as well as the proper number of cameras. At this system of high level apart from the technical installations it is important to have a so-called quick response force that is a manned - human - resource. This must be secured at representations where classified material is handled and no 7/24 hour KBSZCS service is available. A quick response force is secured at these diplomatic missions by readiness or duty service activities. It is important that this force should be available at the site within a very short period of time. Furthermore, the manned service should be able to properly respond to security incidents, i.e. they should in principle and in practice be aware what measures, alarms, etc. should be taken and effected including the possible information and cooperation of the receiving countries' authorities.

Luckily, security incident of physical intrusion into the buildings of a Hungarian diplomatic mission did not often occur. The low number of physical intrusions is probably

due to the technical and manned measures are deterrent to those who want to enter unobserved the premises of the representation.

The present development of ICT means makes it possible that given information can be obtained not only by physical appropriation. Up-to-date electric instruments developed new techniques for the obtention of information, e.g. a modern electronic instrument emits electromagnetic emission that can be copied within a given distance by applying proper instruments. A few decades ago such techniques were only imagined in films but today it is reality. The seriousness of this situation is also proven by the fact that the so-called TEMPEST standard and examination were created. The TEMPEST standard and examination method deals with the regaining and/or hindering the regaining of these data in case of acoustic, electric, magnetic or even light sources, as well. More details of this important national security fact affecting all three territories of electronic information protection (INFOSEC4, COMPUSEC5, COMMSEC6) can be found on pages http://www.tempest.hu/.

Security also means that the adequacy to the regulations must regularly be checked. In the MFA the regular checking of the proper application of these regulations is performed by the Department of Controls, Security and ICT Department as well as by National Security Authority as the competent authority.

Apart from the property protection and handling of classified documents other territories that significantly influence the security level of missions has also to be mentioned. One of these decisive territories was our joining of the Schengen zone. As part of our preparations we had to effect developments at home (at international airports, border crossings etc.) and abroad at our missions in order to meet the Schengen requirements. These developments had to be performed at each mission issuing Schengen visas according to the "Common Consular Instructions" for Schengen countries and the security requirements of the EU Schengen Catalogue. These developments promote as well as maintain the security of visa issuing. In the course of preparation of our Schengen joining at the missions at home and at the MFA the following examples of the development procedure are worth mentioning [9]:

- construction of separate door to the consular section
- introduction of metal detection security control of consular clients
- exchange of traditional glass paneling of consular customer service and certain places for bulletproof windows
- applying up-to-date transfer trays
- installing security cameras
- hiring security guards
- supplying interview rooms with panic buttons
- construction of sluicing-system doors for entering the consulate
- etc.

The security of a consulate can be significantly influenced by the operation of the consular customer service. As a connection a proper informative and queuing system has to be established in order to avoid superfluous queues, lack of information (e.g. necessary documents and data for the administration) and to eliminate possible unpleasant issues. Imagine the situation when a long queue of several ten meters is formed in front of the consulate: unpleasant debates may arise between consular clients concerning who is next, Not to mention that there may be customers with great probability who will not be able to be attended to on the given day due to physical limitations. In case of a properly organized

4 Electronic information protection
5 Computer security
6 Communication security

customer service system this also has to be taken into consideration, because such cases may considerably influence not only the security of the consulate but its vicinity, as well.

Further examples of security technology: there are cases that may occur in Hungary and at our missions, too. It may happen that a peaceful demonstration turns into chaos and if there are no bulletproof windows or windows with special foils, then the building may suffer serious damages or even the people inside, as well. Similar situation can be observed if the fence is not high enough or it can be easily climbed because of its construction. If a panic room7 is available that may keep and increase the feeling of security for a limited time. The level of security can be increased by an automatic alarm system that can call the response force when a burglar or an unauthorized person appears in the court or in the building or a safe box supplied with a time lock that can only be open at a certain time or after a certain period. At certain missions, especially those located at receiving countries fighting against international terrorism, due to public safety requirements it is advisable to procure armored cars or even jeeps and land rovers because of poor road conditions.[8].

At the diplomatic missions, as well at home, a great number of electronic devices are in operation. Due to special conditions in certain countries the power supply is not continuous at some of our missions. Power outage may last long hours or even days, endangering the continuous power supply necessary for everyday work or even the continuous power supply of security instruments. For missions with similar conditions it is advisable to procure a standby power generator. Therefore the procurement of power generators for several missions should centrally be organized by the MFA (e.g. Abuja, Nigeria).

SUMMARY

As it can be stated from the above, although not explained in detail, security technology instruments have become part of everybody's life. In our every day life hardly any situation occurs where we don't meet with some elements of security technology even if we think of the entrance door of our own residence. We should not forget that the hundred percent security does not exist but we can approach this level. Hundred percent well operating security systems do not exist because neither security systems are not completely perfect . Superfluous excitement may be caused by an infra red based motion detector not satisfactorily mounted: e.g. the sensor was turned to watch the window and after sunset or sunset, or when the sun hides behind a cloud the quick drop of temperature may cause an alarm erroneously. This can be eliminated by proper design work. Similar avoidable security event may be caused by the advection of a not properly closed window moving a curtain. The movement sensor may sound off the alarm system after working hours or when nobody is at home because of a movement. Such and similar security incidents/cases/ may be avoided by proper foresight.

For complex security problems our correct answer is: the development, installation and operation of complex security systems. For the installation and operation proper proficiency skills and careful design work is necessary. In order to grant a proper security level of our security systems continuous development and research of security technology, as well as training, retraining and ensuring a second line of experts operating these is also necessary.

7 This is a fortified room, that can protect persons, for hiding in case of break-in, home invasion or even in case of emergency or disaster

List of references

[1] Dr. Kiss Sándor: Biztonságtechnika alapjai – főiskolai jegyzet, ZMNE , 2004

[2] Beyond Fear: Five questions we all ask about security http://www.globalservices.bt.com/InsightsDetailContentAction.do?Record=bruce_schneier_beyond_fear_article_all_en-gb&fromPage=Furl, letöltve: 2011.06.06

[3] 1965. évi törvényerejű rendelet a diplomáciai kapcsoaltokról http://www.mfa.gov.hu/kum/hu/bal/Kulpolitikank/Jogszabalyok/nemzetkozi_dipl_konzuli_jog/Becsi_szerzodes_dipl_kapcsolatok.htm, letöltve: 2011.06.04

[4] Budapesten is megerősítették az amerikai nagykövetség védelmét. http://www.stop.hu/articles/article.php?id=868414,(letöltve: 2011.06.04)

[5] 2134/2004-es (VI.8.) kormányhatározat http://www.mfa.gov.hu/NR/rdonlyres/C151BE5D-2C5F-4643-A525-B0DF6439EF23/0/magyar_kulugyi_evkonyv_2004.pdf, letöltve: 2011.06.04

[6] 2018/2004-es (I.31) kormányhatározat http://uzletinavigator.hu/opten/light/torvtar/torvlist.php?teu=0&twhich=19454, letöltve: 2011.06.07

[7] 90/2010-es (III.26) kormány rendelet http://www.nbf.hu/anyagok/jogszabaly/90-2010%20KormR.doc, letöltve: 2011.06.08

[8] Tájékoztató a közbeszerzésekről http://www.mfa.gov.hu/NR/rdonlyres/57B10362-97CA-4FC7-BCCE-3A0D842A0113/0/átadásátvételpublicjkvmelléklet17.pdf, letöltve: 2011.06.09

[9] 1102/2004-es (XII.23) kormány határozat http://www.solidalapok.hu/sites/default/files/KHA_1102_2007_Korm_hat.pdf, letöltve: 2011.06.04

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Kovács Zoltán
zkovacs@nbsz.gov.hu

FELHŐ ALAPÚ INFORMATIKAI RENDSZEREK POTENCIÁLIS ALKALMAZHATÓSÁGA A RENDVÉDELMI SZERVEKNÉL

Absztrakt

Az elmúlt években egyre többet hallani a felhő alapú számítástechnikáról, vagy cluod computingról. Fel kell tennünk a kérdést, hogy csak a gazdasági alapon működő nagyvállalatok költségcsökkentő és hatékonyságnövelő próbálkozásáról, az IT iparban dolgozó vállalatok gazdasági válság hatásait enyhítendően kitalált új divatszaváról, vagy egy valóban hasznos technológiáról van-e szó? A cikkben példákat hozok jól vagy kevésbé ismert, már működő felhő alapú rendszerekre, áttekintem milyen jellemezőkkel írhatóak le, hogyan csoportosíthatóak, mik azok előnyei, hátrányai. Megvizsgálom mi a különbség a virtualizáció és a felhő alapú rendszerek között, majd választ adok arra a kérdésre, lesz-e felhő alapú rendszer a rendvédelmi szerveknél.

In recent years you could hear more and more about cloud computing. You must ask the question if it is just the large-economy companies' attempt to reduce their costs and increase their efficiency, or it is a new fashion word of the companies of IT industry, using it in order to mitigate the effects of the economic crisis, or it is really a useful technology. In this article I give examples of more or less well-known systems based on cloud computing, overview how they can be described, how they can be sorted, what their advantages and disadvantages are. I examine what the difference is between virtualization and cloud computing, and answer the question if systems based on cloud computing will be used by law enforcement agencies.

Kulcsszavak: *felhő alapú informatika, virtualizáció, szolgáltatási modellek, telepítési modellek ~ cloud computing, virtualization, service models, deployment models*

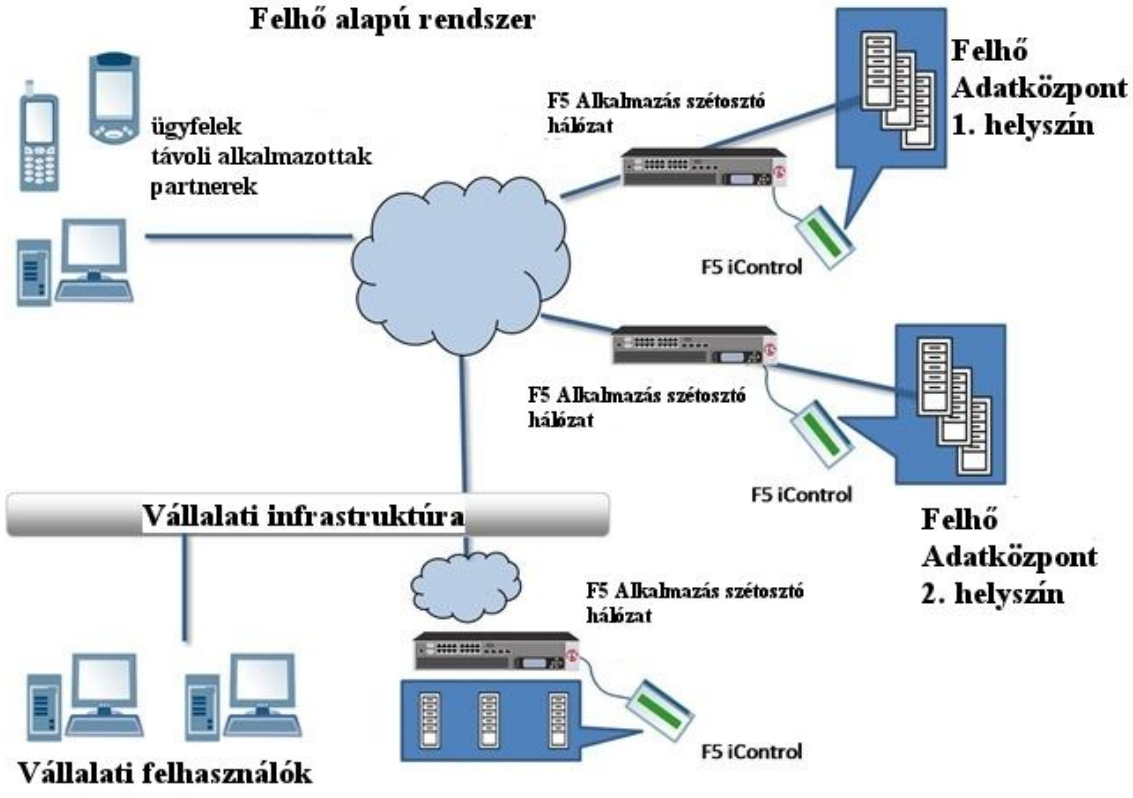
BEVEZETÉS

Az elmúlt évek egyre felkapottabb és ma már talán legdivatosabb információtechnológiai fogalma a „felhő”. Felhő alapú megoldásokról, felhőben tárolt adatokról hallunk, de olvashatunk felhő alapú operációs rendszerről is. Sorra jelennek meg az így működő szolgáltatások, a nagy gyártók ezeket támogató hardveres és szoftveres megoldásai. Neves cégek konferenciákat, előadásokat tartanak róla, itt ismertetve elképzeléseiket, ötleteiket, új, folyamatban lévő, vagy éppen tervezett fejlesztéseiket, felvázolva, hogyan képzelik a – nem is oly távoli – jövőt.

Ha már ennyit hallhatunk, olvashatunk róla, akkor érdemes megvizsgálni, majd megválaszolni – vagy legalábbis megpróbálni megválaszolni – néhány, az állami szervezetek – beleértve a rendvédelmi, nemzetbiztonsági szerveket is – szempontjából lényegesnek tűnő kérdést. Mit is jelent pontosan a felhő alapú informatika? Milyen előnyei, hátrányai vannak? Kell-e, lehet-e használni a rendvédelmi szférában ezt a technológiát? Vagy inkább úgy kell feltennünk ezt a kérdést, hogy meg lehet-e kerülni azok használatát a jövőben? Ezekre a kérdésekre igyekszik a cikk választ találni adni.

Példák felhő alapú rendszerekre, avagy amikkel már találkoztunk vagy találkozhattunk

A felhő alapú információtechnológiai rendszerek lényege, hogy olyan adatokkal, szoftverekkel dolgozunk, amelyek egy része, vagy akár teljes egésze nem saját információtechnológia eszközünkön, hálózatunkon található, hanem valahol az Interneten.[1] Ebben a mondatban a „valahol” a kulcsszó, hiszen nevét is innen kapta ez a technológia. Ezen rendszerek működését bemutató ábrákon ugyanis az hely és az az infrastruktúra, ahol adatainkat, használt alkalmazásainkat stb. tárolják, elérhetővé teszik, számunkra ismeretlen, ezért felhővel szokták ábrázolni (helyettesíteni), mint ahogy azt az 1. ábra is mutatja.



1. ábra. Felhő alapú rendszer ábrázolása
Forrás: http://nxtcloud.blogspot.com/, (letöltve: 2011.10.29.)

Már régóta használunk webes email szolgáltatásokat, amelyek ugyanezen az elven működnek, ez nem szokatlan számunkra. Az utóbbi időben megjelentek a webes tárhelyet kínáló szolgáltatások, szolgáltatók, lelhetővé téve, hogy képeinket, dokumentumainkat, zenéinket is Interneten tároljuk, ezáltal csökkenthetjük a saját eszközeinkben a háttértárak méretét és bárhonnan (ahol Internet elérés biztosított), bármilyen arra megfelelő eszközzel (tehát nem kizárólag a saját számítógépünkkel), bármikor hozzáférhetünk adatainkhoz. Ez mára már annyira elterjedt, hogy pl. a linux alapú Ubuntu operációs rendszerben a 11.04-es, fejlesztői kódnevén a Natty Narwhal változattól már beágyazottan elérhető az Ubuntu One, amely az előzőekhez hasonló szolgáltatásokat kínál. A bárhonnan, bármilyen eszközökkel elérhetőség kritériumát pedig az Ubuntu One szolgáltatója iPhone, Android valamint Windows kliens kiadásával tervezte lefedni, sőt a még rugalmasabb használat érdekében lehetővé tették a névjegyek importálását olyan népszerű alkalmazásokból, mint a Facebook és a Gmail.[2] De hasonló szolgáltatásokat kínál a Windows 7 és a Windows Live kombináció is.[3]

Nem csak adatokat érhetünk el online, hanem – mint már említettem – komplett alkalmazásokat is. Ilyen pl. a Microsoft Office csomagjának online verziója, az ún. Office 365, amely a felhasználóknak a megszokott együttműködési és irodai eszközöket kínálja, felhőalapú szolgáltatások formájában.[4]

A kínálat nem áll meg itt, már olyan alkalmazásokat is „felhősítettek", mint a víruskeresők (például a Panda Cloud Antivirus, amely felhő alapú szolgáltatásának köszönhetően kis méretével és erőforrásigényével kíván nagy népszerűségre szert tenni[5]), de találkozhatunk felhő alapú (hoszting) szolgáltatással a NEXON-tól, amelyben a cég online elérést kínál HR szoftvereihez[6], vagy mobil és felhő alapú nyomtatási szolgáltatásokkal az Epsontól[7].

Az operációs rendszerek fejlesztői is elindultak a felhő alapú, online szolgáltatásként nyújtott forma irányába. Gondoljunk itt a Google régóta dédelgetett tervére a Google Chrome OS-re[8], amely végül 2011. nyarára készült el, és az első kifejezetten erre fejlesztett notebookokkal együtt került forgalomba[9][10], vagy akár az Ubuntu 11.04-es verziójának telepítés nélkül, online, böngészőből kipróbálható verziójára.[2]

A FELHŐ ALAPÚ RENDSZEREK TULAJDONSÁGAI, CSOPORTOSÍTÁSAI, ELŐNYEI, HÁTRÁNYAI

Hosszasan lehetne sorolni a példákat, kiegészítve a listát, bővítve azon szolgáltatások körét, amelyeket felhő alapú szolgáltatás keretében vehetünk igénybe, mégis lehetne még újabbakat találni, és másnapra szinte biztosan megjelenik egy olyan, amelyre még csak nem is gondoltunk. Ugyanakkor lehet rendszerezni is ezeket a szolgáltatásokat, mint ahogyan azt a NIST (National Institute of Standards and Technology) Információtechnológiai Laboratóriuma (Information Technology Laboratory) is megtette.[11] Az alábbiakban az általuk közzétett rendszerezést követve kerülnek csoportosításra a felhő alapú rendszerek, hiszen szinte minden felhő alapú információtechnológiával foglalkozó cikk, blogbejegyzés e szerint a logika szerint teszi meg ugyanezt, és véleményem szerint is ma ez adja a legátfogóbb rendszert. Hozzá kell azonban tenni azt, hogy a NIST munkatársai szerint is egy jelentősen fejlődő technológiáról van szó, ahol a definíciók is idővel fejlődni, változni, finomodni fognak.[12]

Először tekintsük át, hogy mely tulajdonságok megléte esetén mondhatjuk, hogy felhő alapú szolgáltatással van dolgunk:

- Igény szerinti önkiszolgálás (On-demand self service)
- A felhasználók szükségleteik szerint, a szolgáltatónál történő emberi beavatkozás nélkül képesek változtatni az igényelt számítási kapacitásokat, mint például szerver idő, hálózati tárolók stb.

- Jó hálózati hozzáférés (Broad network access)

Hálózaton, szabványos mechanizmusokon keresztül, heterogén eszközökkel (legyen akár vékony vagy vastag kliens pl. mobiltelefonok, laptopok, PDA-k stb.) elérhetőek a szolgáltatások.

- Erőforrás készletek (Resource pool)
- A szolgáltató készletezett erőforrásokat ajánl fel a fogyasztók számára a több bérlős modell szerint, a fogyasztói kereslet szerint dinamikusan kiosztva és újraosztva a fizikai és virtuális erőforrásokat. A felhasználó általában nem ismeri, vagy nem tudja kontrollálni a biztosított erőforrások pontos helyét, csak valamilyen magasabb szinten (pl. ország, állam/megye, adatközpont)
- Teljes rugalmasság (Rapid elasticity)
- A fogyasztónak felkínált kapacitások gyorsan és rugalmasan változtathatóak, fel-, és leskálázhatóak az aktuális igények szerint, a felhasználó számára úgy tűnik, mintha korlátlan mennyiségben állna rendelkezésre.
- Mért szolgáltatások (Measured Service)
- A felhő alapú rendszerek automatikusan, a kívánt szolgáltatások típusának megfelelően képesek vezérelni és optimalizálni a rendelkezésre álló erőforrásokat (pl. tárolás, feldolgozás, sávszélesség, aktív felhasználói fiókok). Az erőforrások megfigyelhetőek, ellenőrizhetőek, használatuk pontosan mérhető, így biztosítva mind a használt szolgáltatás fogyasztója és üzemeltetője számára az átláthatóságot (pontos, mindkét fél számára elfogadott számlázási lehetőséget).[13]

A NIST szakemberei szerint ezek azok a tulajdonságok, amelyek az adott rendszerhez felhasznált – és később ismertetésre kerülő – szolgáltatási és telepítési modelltől függetlenül jellemzik a felhő alapú rendszereket.

Több cikkben, Internetes publikációban találkozhatunk olyan megjelölt tulajdonságokkal (rendelkezésre állás, a kiszolgálás gyorsasága, megbízhatóság, skálázhatóság, teljesítmény, biztonság, karbantartás, költség stb.), amelyekkel a felhő alapú rendszereket próbálják jellemezni. Egy adott felhő alapú rendszer pontos leírásánál véleményem szerint rendkívül fontos a figyelembe veendő tényezők, meghatározó jellemzők pontos kiválasztása. Így azokat a (leendő) felhasználónak mindig az adott esethez, saját igényeihez, elvárásaihoz célszerű összeválogatnia és melléjük fontossági sorrendet felállítania, akár úgy, hogy az egyes tényezők mellé előre megadja hány százalékban kívánja a végző értékelésénél figyelembe venni az adott tulajdonságot.

Ahhoz azonban, hogy a felhő alapú rendszereket csoportosíthassuk, egy ilyen elven működő rendszert pontosan besorolhassunk, szükség van a már említett két modell csoport – a szolgáltatási és a telepítési – kategóriáinak ismeretére is, előnyeikkel, hátárnyaikkal együtt.

Szolgáltatási modellek (Service Models):

- Szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)

A felhasználó számára nyújtott képességeket a felhő infrastruktúrában futó szolgáltatói alkalmazások biztosítják. Az alkalmazások különböző eszközökön, vékony kliens felületen pl. web böngészőn elérhetőek. (ilyen pl. a webmail szolgáltatás). A felhasználó néhány felhasználó-specifikus alkalmazás korlátozott konfigurációs beállítási lehetőségétől eltekintve semmilyen ráhatással sincs a mögöttes infrastruktúrára, hálózatra, szerverekre, operációs rendszerekre, a tárolás módjára, vagy akár egyedi alkalmazások képességére.

Előnyei: gyorsan bevezethető, azonnal használható, a felhasználói oldalról használható eszközök rendkívül széleskörűek, nem igényel nagy beruházást, a legnagyobb költséget kitevő IT üzemeltetési költség jelentősen csökkenthető, a használt szoftverek mindig naprakészek, az alapvető, általános biztonsági funkciókat a szoláltató biztosítja (pl. vírusvédelem), alkalmazásváltás alacsony költséggel, gyorsan végrehajtható.

Hátrányai: nincs testre szabás vagy egyedi igény kiszolgálás, minimális konfigurálási lehetőség áll rendelkezésre, az alkalmazások képességei adottak, új funkció fejlesztése, beillesztése teljes mértékben a szolgáltatótól függ, bevezetéséhez sok betanításra lehet szükség.

- Platform, mint szolgáltatás (Cloud Platform as a Service (PaaS)

Ebben az esetben a szolgáltató által támogatott programnyelveken és eszközökkel a fogyasztó által készített, vagy megszerzett alkalmazásokat a szolgáltató telepíti egy felhő infrastruktúrára. A felhasználó itt sem képes menedzselni vagy ellenőrizni a mögöttes felhő infrastruktúrát, beleértve a hálózatot, szervereket, operációs rendszereket, vagy a tárolókat, de kontrollálja a telepített szolgáltatásokat és az azok fogadására szolgáló környezet konfigurációját.

Előnyei: egyedi, akár saját készítésű szoftverek használhatóak, ezért a bevezetése gyors és egyszerű, a heterogén szoftverkörnyezet bizonyos mértékben homogenizálódik, IT beruházásokra fordított kiadások jelentős mértékben csökkennek, hiszen nem kell rövid idejű csúcsterhelésre méretezett rendszereket vásárolni, karbantartani, a felhasználói oldalon eddig használt eszközök nagy része továbbra is használható.

Hátrányai: felhasználó által telepített alkalmazások naprakészen tartása továbbra is a felhasználó feladata, a telepíthető alkalmazásokat a szolgáltató által biztosított hardver és szoftver komponensek (operációs rendszer) korlátolja, ezért gondos választás esetén is kompromisszumos megoldás születhet, szolgáltatónál történő változások (hardver, szoftver egyaránt) nem tervezett fejlesztéseket indukálhatnak, a felhasználói oldalon magasabb fokú IT háttértámogatást igényel a felhasználó részéről, ezért az IT karbantartásra fordított költségek (beleértve a béreket is) kevésbé csökkenthetőek, mint a SaaS megoldás esetében, a felhasználó által biztosított alkalmazásokat – már amennyiben egyáltalán lehet, vagy gazdaságos – át kell írni ahhoz, hogy a PaaS megoldás előnyeit valóban kiaknázhassuk.

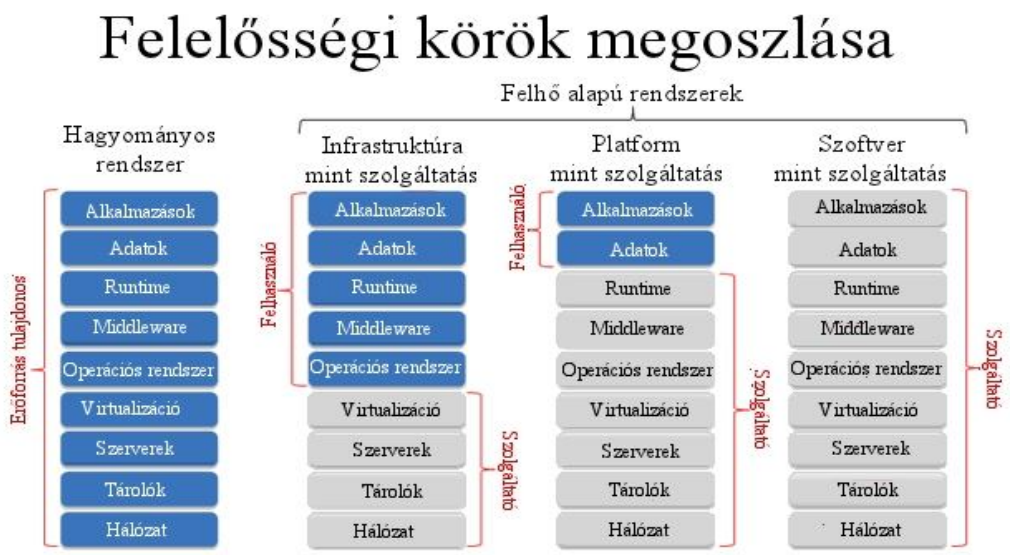
- Infrastruktúra, mint szolgáltatás (Cloud Infrastructure as a Service (IaaS)

A felhasználó számára ebben az esetben olyan számítási, tárolási, hálózati és egyéb alapvető informatikai erőforrásokat biztosít a szolgáltató, amelyre, és amelyen tetszőleges szoftvereket telepíthet és futtathat, beleértve az operációs rendszereket és alkalmazásokat. A felhasználó nem képes menedzselni vagy ellenőrizni a mögöttes felhő infrastruktúrát, de kontrollálni tudja az operációs rendszereket, tárhelyeket, telepített alkalmazásokat, és esetleg korlátozott ráhatása lehet a hálózati elemek (pl. tűzfalak) kiválasztására.

Előnyei: a teljes, megszokott, már testre szabott szoftverkörnyezet átültethető, így betanítás nélkül, a régi eszközökkel használható, könnyen bevezethető, az összes szoftver teljes kontrollja biztosítható (kivéve a virtualizációt biztosítót, de ez talán a legkevésbé kritikus), új szoftverkomponens, funkció bevezetése kizárólag a felhasználótól függ.

Hátrányai: a teljes szoftverkörnyezet kialakítása, karban-, és napra készen tartása a felhasználót terheli, felhasználói oldalon szinte ugyanazt az informatikai szervezetet fenn kell tartani, mint korábban, konzerválódhat a régi, elavult, heterogén szoftverkörnyezet, a három modell közül ezzel csökkenthetőek legkevésbé az korábbi IT költségek.[14]

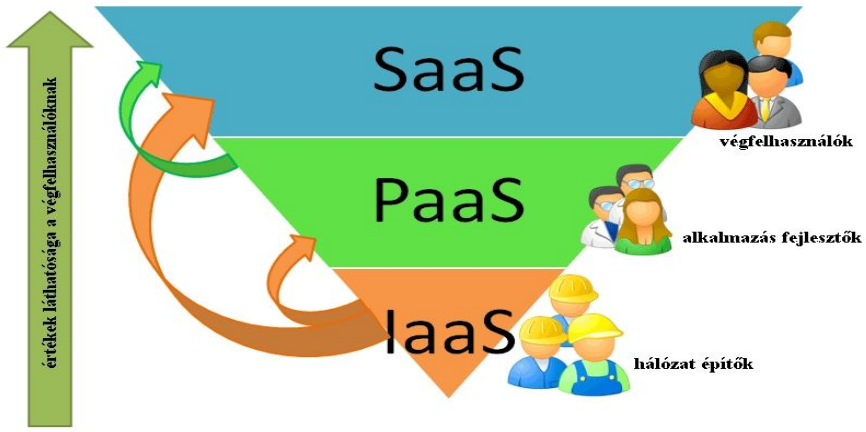
Az egyes modelleknél a felhasználó és a szolgáltató felelősségi körébe tartozó feladatokat jól szemlélteti az 2. ábra. Az Interneten ezzel a kérdéskörrel foglalkozó cikkek, blogok vagy ugyanezt a felosztást, vagy ehhez nagyon hasonlót használnak, de lényeges eltérés ezek között nem található.



2. ábra. Felelősségi körök megoszlása a szolgáltatási modellekben
Forrás: http://blogs.cisco.com/wp-content/uploads/Seperation-of-Responsibility-in-Cloud.png, (letöltve: 2011.10.29.)

A szolgáltatási modelleket már többen, többféleképpen megpróbálták kiegészíteni (mint ahogy már utaltam rá, a NIST szakemberei is hasonló fejlődési folyamatot várnak). Megjelentek az olyan fogalmak, mint a Desktop as a service (DaaS)[15] (amely vékonykliensek kiszolgálására használt desktop rendszerek virtualizációját jelenti) vagy a PRaaS (Process as a service)[16] (amely szerint a teljes folyamat egy komplett, felhőben futó megoldás, úgy, hogy a felhasználónak nincs szüksége semmilyen IT szakember beavatkozására). De amíg a fent kifejtett 3 modellt teljes mértékben mindenki – beleértve az ipari szereplőket is – elfogadja és – ha úgy tetszik – kvázi-szabványként használja, addig az utóbbiak (és az itt fel nem soroltak is) vagy nem ismertek, vagy nem elfogadottak és megkérdőjelezik a létjogosultságukat.[17]

A 3. ábrán láthatjuk, hogy kik értékelik, látják igazán az adott szolgáltatási modellek előnyeit.



3. ábra. A szolgáltatási modellek előnyeinek értékelői
Forrás: http://www.saasblogs.com/saas/demystifying-the-cloud-where-do-saas-paas-and-other-acronyms-fit-in/, (letöltve: 2011.10.29.)

Telepítési modellek (Deployment Models):

- Magán számítási felhő (Private cloud)

A felhő infrastruktúra kizárólag egy szervezet számára működik. Ezt akár a felhasználó szervezet, de akár egy másik fél is menedzselheti, fizikailag lehet akár a felhasználó telephelyén, akár azon kívül.

Előnyei: a teljes rendszer kézben tartott, a biztonság itt garantálható a legjobban, meglévő rendszerek, rendszerelemek felhasználhatóak.

Hátrányai: korlátozott erőforrások, csúcsterhelésre kell tervezni, kevésbé skálázható, a korábbi IT-re fordított költségek csökkentése itt érhető el a legkevésbé.

- Közösségi számítási felhő (Community cloud)

Ebben az esetben a felhő infrastruktúrát több szervezet megosztottan használja, úgy, hogy az, az adott közösség közös érdekeit támogassa (pl. közös küldetés, biztonsági követelmények, előírások, megfelelőségi szempontok). Ezt menedzselheti akár a felhasználó szervezet, akár egy másik fél is, fizikailag lehet akár a felhasználó telephelyén, akár azon kívül.

Előnyei: a közös érdekek okán az adott feladatokra jól skálázható, jelentős költség takarítható meg, hiszen az erre fordítandó IT költségek megoszlanak, a biztonság megfelelően garantálható, a közös érdekek szerinti kritériumoknak tökéletesen megfeleltethető.

Hátrányai: közös érdekek mellet is lehetnek egyedi igények, ezek bizonyos esetekben csak kompromisszumokkal vagy egyáltalán nem teljesülnek, limitált skálázhatóság (közös érdekeknél azonos időben jelentkezhetnek csúcsterhelések, ami kritikus lehet, vagy éppen a költségcsökkenési előnyt veszíthetjük el), adott esetben az addig használt szoftverek, alkalmazások cseréje szükséges.

- Nyilvános számítási felhő (Public cloud)

A felhő infrastruktúra ebben a modellben bárki (a nagyközönség vagy egy nagy (ipari) csoport) számára elérhető, de a felhőszolgáltatást nyújtó szervezet tulajdonában van. A példákról szóló fejezetben szinte csak ilyenekről szóltam, ez tekinthető ma a legismertebb telepítési modellnek.

Előnyei: teljes felhasználói mobilitás biztosított, jól skálázható, legtöbb költség itt takarítható meg, csak annyit kell fizetni, amennyit fogyasztunk, szinte karbantartásmentes, itt szükséges a legkisebb létszámú IT csapat a felhasználónál.

Hátrányai: problémák lehetnek az elérhetőséggel, az adatvisszaállítással, kiszolgálással, nem ismert az infrastruktúra fizikai elhelyezkedése, a biztonság itt garantálható a legkevésbé.

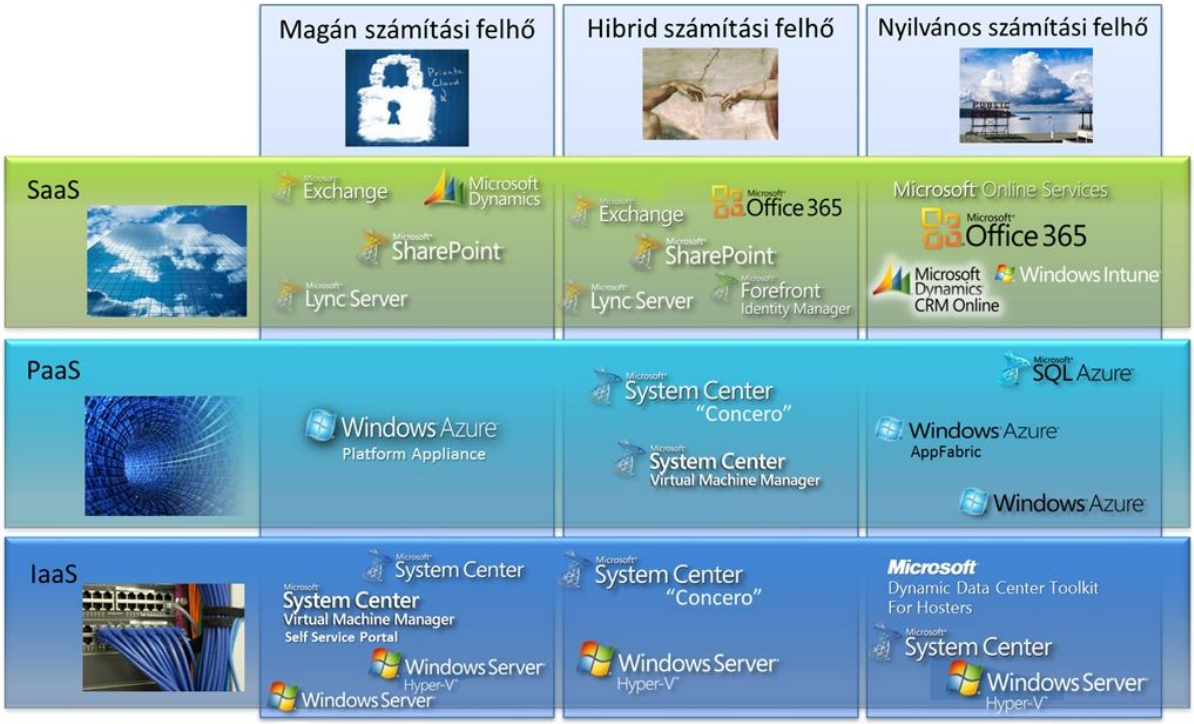
- Hibrid számítási felhő (Hybrid cloud)

A felhő infrastruktúra ekkor több, az előző modellek szerint felépülő rendszer (magán, közösségi, nyilvános) keveréke, ahol a felhők megtartják egyedi jellegzetességeiket, azokat szabványosított vagy szabadalmazott technológiák kötik össze, lehetővé téve az adatok és alkalmazások hordozhatóságát (pl. cloudbursting technológia a felhők közötti terhelés-kiegyenlítésre, amikor a magán felhőben rendelkezésre álló erőforrások elfogynak és azokat más, tipikusan nyilvános felhőben meglévőkkel pótolják ki [18]).

Előnyei: alapvetően kézben tartott rendszer, amely egyedi igények szerint épül fel, az átlagterhelés feletti szükséges plusz kapacitásokat igény szerinti mértékben és időtartamban kell csak megvásárolni, a nem csúcsra méretezett IT rendszerek okán költségek takaríthatók meg.

Hátrányai: összekapcsoláskor nem biztosított homogén módon a rendelkezésre állás, az adatvisszaállítás és a biztonság, nem, vagy csak korlátozottan rendelkezünk ismeretekkel a saját rendszeren kívüli többi erőforrás fizikai helyét, összetételét, biztonságát stb. illetően.[19].

A szolgáltatási és a telepítési modellekből egyfajta mátrix képezhető. Ebben a mátrixban kell megtalálnia a felhasználónak, hogy hová helyezi saját (meglévő vagy tervezett) hálózatát, és ennek mezőibe pozícionált termékek közül tudja kiválasztani a számára megfelelőket. Egy ilyen termékpozicionálást mutat a 4. ábra, itt most a Microsoft termékeire.



4. ábra. Termékpozicionálás a szolgáltatási-telepítési modell mátrixban
Forrás: http://lepenyet.wordpress.com/2011/06/29/a-szmtsi-felhok-hatsa-az-it-versenyhelyzetekre/, (letöltve: 2011.10.28.)

VIRTUALIZÁCIÓ VS. FELHŐ

Az előző fejezetek ismertették, hogy mit takar a felhő alapú rendszer kifejezés, milyen kategóriákba oszthatjuk őket és milyen tulajdonságokkal jellemezhetőek. Felmerülhet azonban az a kérdés, hogy mi a különbség a felhő és a ma szintén oly divatos virtualizáció között.

Összefoglalóan azt mondhatjuk, hogy virtualizációról akkor beszélhetünk, ha egy olyan infrastruktúrát hozunk létre, ahol az erőforrások elosztását rugalmasan, a szükségleteknek megfelelően végezhetjük el, oly módon, hogy az adott informatikai erőforrást a többi erőforrástól elkülönítetten vagy leválasztottan kezeljük.[20][21]

Miért erőforrásokat említettem? A mai – elterjedt – technológiákat tekintve és rendkívül leegyszerűsítve a dolgot azt mondhatnánk, hogy virtualizáció az, amikor egy adott hardveren több virtuális rendszert működtetünk.[22] Ennél azért jóval többről van szó, hiszen a virtualizáció az adatközponttól a munkaállomásig az informatika minden rétegére lehet alkalmazni.[20] A 5. ábra jól szemlélteti a teljes „hagyományos” informatika és a teljes virtualizáció közötti technikai különbségeket, minden rétegen.

5. ábra. A „hagyományos” és a virtualizált informatika közötti különbségek
Forrás: http://www.microsoft.com/hun/virtualization/promise.mspx, (letöltve: 2011.10.28.)

A felhő alapú rendszerekhez hasonlóan a virtualizált környezetben sem tudja a felhasználó megmondani, hogy az általa futtatott alkalmazások milyen fizikai hardveren futnak, vagy éppen az adatai hol kerültek tárolásra. Akkor mi a különbség a felhő és a virtualizáció között? Ha most is egyszerűen akarjuk megfogalmazni, akkor az emberi beavatkozás szükségességét jelölhetjük meg alapvető különbségként. Egy virtualizált rendszer beállításához, felügyeletéhez, ellenőrzéséhez, karbantartásához a felhasználónál nagyobb informatikai háttér szükséges, mint nem virtualizált esetben, hiszen a virtualizált termékek nem helyhez kötöttek, a fizikai futtatásuk helyszíne nehezebben behatárolható, és jóval nagyobb, mint felhő alapú rendszer használata esetén, ahol ezt a problémát a felhő alapú rendszer szolgáltatója átveszi a felhasználótól.

A virtualizáció is – a felhő alapú rendszerekhez hasonlóan – lehetővé teszi az erőforrások a „hagyományos” informatikai megoldásokhoz képesti jobb kihasználását, ám azok elosztásához, újraosztásához emberi beavatkozás szükséges, míg a felhő alapú rendszerek esetében ez automatikus, emberi beavatkozás nélkül zajlódik le.[23] Virtualizált környezet kezdeti beállításánál bizonyos mennyiségű erőforrást rendelünk adott alkalmazásokhoz, majd ha valamelyik erőforrásigénye egy kritikus szintet elér, akkor ismételt emberi beavatkozással rendelhetünk hozzá újabb erőforrásokat. Ez nem csak az emberi beavatkozás szükségességét vetíti elénk, hanem azt is, hogy a felhő alapú rendszerekben az erőforrások felhasználása hatékonyabb, újraosztása gyorsabb, a kritikus leállások - pl. erőforráshiány miatt – száma kevesebb lehet.

A virtualizációra tehát tekinthetünk úgy, mint a klasszikus viccben az alkoholmentes sörre, azaz ha már használunk valamilyenfajta virtualizációt, akkor az első lépést megtettük a felhő alapú rendszerek alkalmazása felé, ám ez utóbbiak összes előnyét még nem élvezhetjük.

RENDVÉDELMI SZERVEK ÉS A FELHŐ, AVAGY LESZ-E ITT FELHŐALAPÚ RENDSZER?

Tarot kártya, üveggömb, kávézacc nélkül nehéz megjósolni a jövőt, de az IT ipar tendenciáiból, az erre szakosodott cégek előrejelzéséből viszonylag jó következtetéseket lehet levonni. Nézzük először is, hogy mi várható a felhő alapú rendszerekkel kapcsolatban globálisan.

Az IDC szerint a felhő alapú rendszerek és a hozzájuk kapcsolódó szolgáltatások szegmense átlagosan évi 28 százalékkal nő majd, így a 2011-ben mintegy 21,5 milliárd

dolláros piac 2015-re 73 milliárd dollárosra bővül. De nem csak ezt, hanem a teljes IT iparág átalakulását, átrendeződését is jósolják az IDC szakértői, véleményük szerint ez a technológia – összefonódva a egyre okosodó és terjedő mobil eszközökkel, valamint közösségi hálózatokkal – adja majd az iparág harmadik nagy platformját és hozza el a mainframe-ek és a PC-k utáni a harmadik nagy növekedési hullámot.[24]

Egy másik elemzésben a Gartner piacelemző cég szerint 2012-re a legnagyobb, Fortune 1000 soraiba tartozó vállalatok 80 százaléka igénybe fog venni valamilyen felhőalapú szolgáltatást.[25]

A Cisco Connected World Report című 2010. december 8-án megjelentetett nemzetközi tanulmánysorozat harmadik részében 13 országra kiterjedő vizsgálat adatait tették közzé – többek között – a felhő alapú rendszerek jelenlegi felhasználásával, valamint azok tervezett bevezetésével kapcsolatosan. A válaszok szerint a megkérdezettek 18% már használ valamilyen felhőalapú megoldást, 34% pedig tervezi bevezetését. 92% vélekedett úgy, hogy a következő három évben adataihoz és alkalmazásaihoz bizonyos részben privát vagy nyilvános felhőrendszert vesz majd igénybe.[26]

Az ipar szereplői is komolyan veszik a felhő alapú rendszereknek jósolt kiemelkedő jövőt. Senki sem szeretne lemaradni, a jelenlegi nagyok meg kívánják őrizni vezető szerepüket, a kihívók, vagy új piaci szereplők pedig ebben látják a nagy lehetőséget az előrelépésre. Számos példát ismerünk arra, hogyan bukhatnak, vagy maradhatnak le a nagyok, ha korábbi sikeres termékeiket, technológiájukat erőltetik, azokkal akarják megtartani pici előnyüket (pl. IBM[27], Nokia[28]).

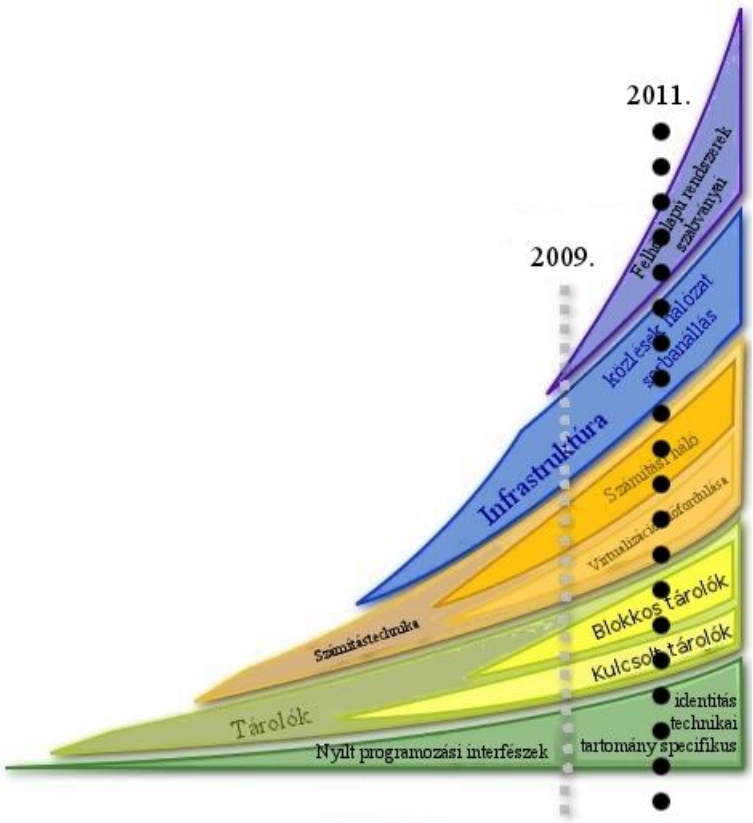
Jó példa a vezető szerep megtartására való törekvésre a Microsoft, amely - Steve Ballmer a Microsoft vezérigazgatója szerint - máig közel 10 milliárd dollárt fektetett a felhő alapú rendszerek kutatásába és fejlesztésébe.[29]

Tovább lehetne sorolni a példákat, kiegészítve más elemzésekkel, újabb piaci szereplőkről szóló adatokkal, de már ez is plasztikusan mutatja, hogy a következő évek az IT világában a felhőről fognak szólni. Nem mehetnek el e mellett az állami intézmények, így a rendvédelmi szervek sem. A felhő alapú rendszerek előnyei (költség megtakarítás, skálázhatóság, könnyebb üzemeltetés stb.), valamint az elhúzódó gazdasági válság államra gyakorolt hatása (pl. állam fenntartására fordítható kiadások csökkenése) olyan hívószavak, amelyek tovább erősítik az iparági tendenciákat és e hatékonyabb technológia felhasználása irányába hatnak.

A következőben két idézetet hozok. Az egyik Steve Ballmer a Microsoft vezérigazgatója által 2010. november 18-án írt cikkből való: *„Az üzleti élet mellett a közigazgatás szereplői is felismerték az új technológia előnyeit. Európa kormányaival és állami intézményeivel együttműködve azon dolgozunk, hogy kitaláljuk, miként növelhető a hatékonyság a felhő alapú megoldásokkal, miként nyújthatók jobb szolgáltatások, illetve hogyan fokozható a növekedés. Látható, hogy a felhő alapú számítástechnikának köszönhetően Európa polgárai mára hatékonyabb és gyorsabb közigazgatási szolgáltatásokban részesülnek, s a közszférában is teret nyer a vállalkozói szellem, a dinamizmus és a kísérletező kedv.”*[29]

A másik Kalotay Balázs, a Fujitsu Technology Solutions Kft. szakértőjének az „Új típusú IT funkciók az új gazdasági környezethez” címmel Budapesten megrendezett IDC Hosting Konferencián tett megállapítása: *„Minden korábbinál nagyobb szükségük van a magyar önkormányzatoknak, valamint a kis- és középvállalatoknak a felhő alapú számítástechnikai szolgáltatásokra, A válság időszakában ugyanis a magyar gazdaság legtöbb szereplőjének nem áll rendelkezésére elegendő fejlesztési forrás informatika rendszerük színvonalának szinten tartására a hagyományos módon. Ebben a helyzetben a megoldást az infrastruktúra beruházások költségét minimalizáló és a működési kiadásokat csaknem megfelező felhő szolgáltatások igénybevétele jelentheti. Számos városi és járási (kistérségi) önkormányzat, valamint jó néhány vállalat már felismerte ezt a lehetőséget és élvezi a Fujitsu technológiája által nyújtott előnyöket.”*[30]

2011 tavaszán arról is jelent meg publikáció, hogy Magyarországon elsőként Veszprém, másodikként Fejér megye csatlakozott a felhő alapú szolgáltatásokhoz.[31] Ez jól mutatja, hogy az állami szférában is megkezdődött a „felhő korszak”.



6. ábra. A felhő alapú rendszerek növekedési előrejelzése
Forrás: http://www.zdnet.com/blog/hinchcliffe/cloud-computing-and-the-return-of-the-platform-wars/303?tag=mantle_skin;content, (letöltve: 2011.10.28.)

A 6. ábra mutatja, milyen növekedést jósolt a felhő alapú számítástechnikának Dion Hinchcliffe 2009. március 26-án blogjában. A szürke szaggatott vonal jelzi, hogy Hinchcliffe szerint hol tartottunk a témában 2009-en. A főbb területek kategorizálása, azok egymáshoz viszonyított aránya véleményem szerint ma is helytálló, meglátásom szerint azonban napjainkban már a 2011. címkéjű szaggatott vonalnál járunk.

Tehát csontvetés és jós inga nélkül is kijelenthető, a kérdés nem az, hogy lesz-e a rendvédelmi szektorban felhő alapú rendszer, még csak nem is az, hogy minden szervezet használni fogja-e. Ezekre a válasz már megszületett. A kérdés sokkal inkább az, mikortól, milyen formában, milyen feltételek mellett. Válaszokat kell találni továbbá a biztonsági kérdésekre, hiszen ezek egyrészt ilyen jellegű felhasználás esetén sokkal kritikusabb tényezők, mint magán, vagy más állami, önkormányzati stb. felhasználás esetén, másrészt ma ez a felhő alapú rendszerek egyik legfőbb problémája.

Biztonsági kérdések megfogalmazás persze egy rendkívül nagyvonalú egyszerűsítés. Itt olyan kérdéseket kell megvizsgálni a valódi biztonsági kérdéseken kívül, mint adatvédelem, megfelelőség, jogi és szerződéses kérdések, de ezeket a kategóriákat is tovább kell bontanunk, a biztonságon belül pl. adatvédelmi, üzemeltetési integritási, sérülékenységi, személyazonosság-kezelési stb. kérdéseket kell boncolgatnunk.[32] Meg kell határozni, hogy ezek közül melyek azok, amelyeket egy felhő alapú rendszernél vizsgálni szükséges, azokat pontosan definiálni kell, át kell tekinteni, hogy ezek közül melyek és milyen mértékben relevánsak a rendvédelmi szervezetek számára. De ez már egy másik cikk témája.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Jelen cikk több példát is bemutatott a felhő alapú rendszerekre, áttekintette milyen jellemezőkkel írhatóak le, milyen elfogadott modellek léteznek, azok mentén hogyan csoportosíthatóak az ilyen elven működő rendszerek, melyek azok előnyei, hátrányai. Megvizsgálta mi a különbség a virtualizáció és a felhő alapú rendszerek között, mi a felhő alapú informatika előnye a virtualizációhoz képest, majd választ adott arra a kérdésre, lesz-e felhő alapú rendszer a rendvédelmi szerveknél.

Összefoglalásként elmondható, hogy a felhő alapú informatikai rendszerek megjelenése és használata megkerülhetetlennek tűnik a rendvédelmi szervek esetében. A fent említett nagy iparági beruházások nyomán kialakult, kialakuló sok fajta és széles szolgáltatási palettát kínáló felhő alapú informatika az eddigieknél olcsóbban képes a jelenlegi számítástechnikai igények kielégítésére, vagy akár a meglévőknél több, újabb feladat ellátására. Ez és a rendvédelmi szervek rendelkezésére álló, behatárolt IT-re fordítható költségvetés olyan hívószavak, amelyek miatt a felhő alapú rendszerek bevezetése biztosra vehető. Ugyanakkor ez a szimpla megállapítás újabb kérdéseket vet fel (pl. biztonság tekintetében), amelyeket meg kell válaszolni, mielőtt fejest ugrunk az ilyen rendszerek tervezésébe, kiépítésébe.

Át kell tekinteni, hogy a felhő alapú rendszerek milyen biztonsági jellemzőkkel írhatók le, azokat csoportosítani és pontosan definiálni kell. Ezek után kell meghatározni a rendvédelmi szervek számára relevánsakat, majd a szolgáltatási-telepítési modell mátrixból kiválasztani azt, amely biztosítja, hogy a kívánt IT szolgáltatásokhoz a megfelelő biztonság mellett a jelenleginél olcsóbban jussunk hozzá. A kiválasztás után pontosítani kell az elvárt üzem-, és adatbiztonsági kritériumokat, és azokat olyan technikai és jogi megoldásokkal körülbástyázni, amely lehetővé teszi, hogy egy adatot az, és csak az érhessen el, aki arra jogosult, ő viszont midig, amikor szükséges, az adat teljes életciklusában. Különös tekintettel kell lenni arra, hogy harmadik fél illetéktelenül ne férhessen hozzá az adatokhoz (és ez sokszor nem, vagy nem csak a szolgáltató feladata), ugyanakkor adott esetekben a törvényes monitoringot biztosítani kell.

Felhasznált irodalom

[1] http://pcworld.hu/hogyan-szerezzunk-felho-alapu-virusirtot-tuzfallal-20110916.html, (letöltve: 2011. 10. 04.)

[2] http://ubuntu.hu/ubuntu1104/press, (letöltve: 2011.10.21.)

[3] http://windows.microsoft.com/hu-HU/windows/cloud, (letöltve: 2011.10.22.)

[4] http://www.microsoft.com/hu-hu/office365/how-office365-works.aspx, (letöltve: 2011.10.21.)

[5] http://pcworld.hu/hogyan-szerezzunk-felho-alapu-virusirtot-tuzfallal-20110916.html, (letöltve: 2011. 10. 04.)

[6] http://www.nexon.hu/felho-alapu-hoszting-szolgaltatas, (letöltve: 2011. 10. 07.)

[7] http://hirek.prim.hu/cikk/2011/09/14/tovabbfejlesztett_mobil_es_felho_alapu_nyomtatasi_szolgaltatasok_az_epsontol, (letöltve: 2011. 10. 07.)

[8] http://hu.wikipedia.org/wiki/Chrome_OS, (letöltve: 2011.10.21.)

[9] http://www.hwsw.hu/hirek/45786/google-chrome-os-web-store-bongeszo-operacios-rendszer-notebook-netbook.html, (letöltve: 2011.10.21.)

[10] http://www.google.com/chromebook/, (letöltve: 2011.10.21.)

[11] http://www.nist.gov/itl/cloud/index.cfm, (letöltve: 2011.10.21.)

[12] P. Mell, T. Grance : *The NIST Definition of Cloud Computing Version 15*, 10-7-09, National Institute of Standards and Technology, Information Technology Laboratory (ww.nist.gov/itl/cloud/upload/cloud-def-v15.pdf), (letöltve: 2011.10.21.)

[13] http://lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/, (letöltve: 2011.10.21.)

[14] http://lepenyet.wordpress.com/2011/06/16/szmtsi-felho-egyszeruen-2-rsz/, (letöltve: 2011.10.21.)

[15] http://cloudcomputing.sys-con.com/node/1048046, (letöltve: 2011.10.09.)

[16] http://nauges.typepad.com/my_weblog/2009/08/praas-process-as-a-service.html, (letöltve: 2011.10.22.)

[17] http://www.zdnet.com/blog/virtualization/fourth-type-of-cloud-computing/1346, (letöltve: 2011. 10. 09.)

[18] http://cloudsecurity.trendmicro.com/what-is-cloudbursting/, (letöltve: 2011.10.22.)

[19] http://lepenyet.wordpress.com/2011/06/17/szmtsi-felho-egyszeruen-3-rsz/, (letöltve: 2011.10.21.)

[20] http://www.microsoft.com/hun/virtualization/promise.mspx, (letöltve: 2011.10.28.)

[21] VASVÁRI GYÖRGY CISM c. egyetemi docens: *AZ IT VIRTUALIZÁCIÓ (AJÁNLÁS 4.0)* 2008 (www.infota.org/biztmen/docs/A_VIRTUALIZACIO_Ajanlas_4.doc), (letöltve: 2011.10.28.)

[22] http://www.kvint-r.hu/termekek_szolgaltatasok/57/virtualizacio_vmware, (letöltve: 2011.10.28.)

[23] http://computerworld.hu/vmware-a-felhokben.html, (letöltve: 2011.10.28.)

[24] http://www.hwsw.hu/hirek/46921/felho-cloud-idc-piac.html, (letöltve: 2011.10.22.)

[25] http://www.isidorcloud.hu/cloud-computing-felhoalapu-szamitastechnika.html, (letöltve: 2011.10.07.)

[26] http://newsroom.cisco.com/dlls/2010/ts_101910.html, (letöltve: 2011.10.28.)

[27] http://lepenyet.wordpress.com/2011/06/29/a-szmtsi-felhok-hatsa-az-it-versenyhelyzetekre/, (letöltve: 2011.10.23.)

[28] http://www.168ora.hu/buxa/csokkent-a-nokia-piaci-reszesedese-80570.html, (letöltve: 2011.10.23.)

[29] http://www.microsoft.com/hun/news/rolunkirtak/101118_01.aspx, (letöltve:2011. 10. 09.)

[30] http://hirek.prim.hu/cikk/79490/, (letöltve: 2011. 10. 07.)

[31] http://www.naplo-online.hu/kronika/20110330_felho_szolgaltatas, (letöltve: 2011. 10. 07.)

[32] http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html, (letöltve: 2011.10.23.)

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Kun István - Fáy Gyula - Bukovics István
kunistvan47@gmail.com - k.profes@chello.hu - bukovicsistvan@wjlf.hu

LOGIKAI HADVISELÉS - KRITIKUS PONTOK HARCA

Absztrakt

A jelen tanulmány egy hosszabb kutatómunka fontos állomását ismerteti. Csatlakozva olyan korszerű hadviselési elvekhez, mint a hálózat-alapú és az entrópia-alapú hadviselés, egy általános logikai modellel foglalkozik, amely nemcsak hadműveletek, hanem a pontosan ki nem számítható külső kockázatnak kitett szervezett tevékenységek sikeres megtervezését és lebonyolítását segíti elő. Az elméleti modellt szemléletes, könnyen kezelhető számítógépes program támogatja. A tanulmány részletesen kifejti az elméleti modellt és képet ad a számítógépes megvalósításról is. Konkrét példával illusztrálja a felhasználás módját és lehetőségeit.

The present study outlines an important station of a long-range research work. Joining up-to-date warfare principles, such as network-centric warfare and entropy-based warfare it is involved in a general logical model supporting not only military manoeuvres but also successful planning and running of organised activities exposed to exactly not calculable outer risks. The theoretical model is supported by a suggestive, easily tractable computer program. The study gives a detailed description of the theoretical model and also demonstrates the computer implementation. Way and options of utilization are illustrated by a concrete example.

Kulcsszavak: *hálózat-alapú hadviselés, logikai model, tervezés ~ network-centric warfare, logical model, planning*

ELŐZMÉNYEK

A hadviselés a technológia általános fejlődésével túllépett azon a szinten, amely a napóleoni típusú tömeghadseregek, majd ehhez csatlakozva a tüzérség, még később pedig a bombázó repülőgépek által szolgáltatott nyers rombolóerőn alapult. Az ilyen típusú hadviselés kényszerűen az érdemi célpontok óriási környezetének elfoglalásával és/vagy teljes elpusztításával járt. Korlátaira a vietnami háború hívta fel a figyelmet: a hatalmas amerikai hadigépezet pusztító ereje sem tudta megtörni az észak-vietnami hadsereget.

A következő fejlődési szintet a múlt század utolsó harmadában a platform-alapú precíziós hadviselés jelentette. Ennek koncepciója: bár központi tervekből kiinduló, de különálló harci egységek illetve fegyverrendszerek által végrehajtott, nagy pontosságú, egyedi döntéseken alapuló csapásokkal kiiktatni az ellenség szervezett, hatékony cselekvését lehetővé tevő eszközöket. Itt a hangsúly az egyedi döntéseken alapuló egyedi végrehajtáson van.

A továbblépés a XX. század kilencvenes éveiben történt. A katonai tervezők és vezetők rájöttek, hogy a saját és az ellenséges erőket egyaránt rendszerként kell kezelni. A saját erők esetében a rendszer nyújtotta hatékonysági előnyöket kell kihasználni, az ellenség esetében pedig ezeknek az előnyöknek a kihasználását kell lehetetlenné tenni. A rendszerelvű hadviselésre két koncepció született.

A hálózat-alapú hadviselést katonai elvként Jay Johnson tengernagy, az USA haditengerészetének hadműveleti parancsnoka említette először az Egyesült Államok Haditengerészeti Intézetében rendezett konferencián 1997-ben (Johnson, 1997). Az elv részletes kifejtése a (Cebrowski-Garstka, 1998), valamint a (Garstka-Alberts-Stein, 1999) publikációkban történt. Lényegét az a felismerés képezte, hogy a bármilyen korszerű technológiát használó egyedi csapásmérés hatékonysága csekély, ha nem az időközben kikristályosodott hálózati szemléleten alapszik. A hálózat, mint működési mód itt mind a saját, mind az ellenséges erők harci potenciáljának figyelembevételénél kulcsfontosságú. A fent vázolt hadviselési paradigmaváltást tárgyalja (Dunn *et al*, 2004).

Ezzel nagyjából egyidőben alakult ki az entrópia-alapú hadviselés elve. Először egy nem publikus (Arquilla-Ronfeldt, 1995), majd egy publikus tanulmányban (Herman, 1997) jelent meg. Az elv szerint az ellenség rendezetlenségét (azaz entrópiáját) kell megnövelni a kohéziót biztosító szervezeti elemek (személyek, eszközök, objektumok) kiiktatásával addig a szintig, hogy a személyi állomány már ne legyen képes a szervezett ellenállásra.

A hálózat-alapú és az entrópia-alapú hadviselés egyaránt arra törekszik, hogy az ellenség rendszerének fontos élő vagy technikai elemeit likvidálja. Az utóbbi évek aszimmetrikus háborúinak tapasztalatai azonban azt mutatják, hogy kulcsfontosságúnak ítélt fizikai célpontok sorának fizikai likvidálása sem mindig elég a rendszer tartós megbénításához.

LOGIKAI HADVISELÉS

A hadviselés logikai modelljéről először a (Cebrowski-Garstka, 1998) tanulmány tesz említést, ezen a különböző hálózatok kooperatív felhasználását érti. Jelen cikkben ettől eltérő jelentést használunk, amelyet a későbbiekben fejtünk ki.

A nemkívánatos események (pl. háborús veszteségek, természeti és civilizációs katasztrófa-jelenségek) és az ellenük való védekezés egzakt tudományos vizsgálatához mindenekelőtt a szemléleti modell legfontosabb elemeit szükséges rögzíteni. Ezért bizonyos feltevésekből indulunk ki. A felhasznált és kidolgozott fogalmak kifejtésére a továbbiakban kerül sor.

A logikai hadviselés koncepcióját a logikai kockázatelemzésre építjük. Erre közelítőleg a "logikai értékelemzés" kifejezést használhatjuk, lásd (Quine, 1968). Ennek az alkalmazott logikában általánosan elterjedt módszernek a logikai kockázatelemzés viszonyára leszűkített esetét a következő alapfogalmak, főszabályok és alapelvek jelentik.

Nemkívánatos esemény, nemvalószínűségi esemény

Eredetileg a *nemkívánatosság* fogalma szigorúan véve nem annyira tudományos, mint inkább morális, etikai. Nem az *igaz-hamis*, hanem a *jó-rossz* dilemmájához kötődik. Tudományossá akkor válik, ha azt vizsgáljuk: adott körülmények között *igaz-e, hogy bekövetkezik egy nemkívánatos esemény*, fennáll-e egy nemkívánt tény. Itt nem arról van szó, hogy meghatározzuk, miben áll a „nemkívánatosság", hanem ennek szükséges és elegendő feltételeit vizsgáljuk.

Mindenesetre a „nemkívánatos" ellentétét nem fogjuk összemosni a kívánatossal.

A nemkívánatos események a legszorosabban összefüggnek a kockázatos eseményekkel, azaz a *kockázati rendszereken* bekövetkező eseményekkel. A kockázatos (más szóval a bizonytalan kimenetelű) eseményeknek *kockázati tényezőik* vannak. A nemkívánatos eseményt mindig egy úgynevezett *kockázati rendszerre* vonatkozóan fogjuk fel. A kockázati rendszer valamely esemény (folyamat, történés, tény) kockázati tényezőinek, valamint e tényezők között értelmezett bizonyos logikai összefüggéseknek az együttesével jellemezhető. A kockázati tényezők maguk is események, pontosabban *tények*. A logikai szigorúság megköveteli, hogy „be nem következett esemény"-ről és „fenn nem álló tény"-ről is beszéljünk. Eseményekről, illetve tényekről és ehhez hasonlókról szólva mindig *ezekre vonatkozó állításokra*, *kijelentésekre* gondolunk, és ezekre a kijelentésekre a (szimbolikus vagy formális) logika szabályait tekintjük érvényesnek (Lsd. (Quine, 1968)).

A nemkívánatos esemény közismert és ma talán egyik legjelentősebb példája a 2001. szeptember 11-i New York-i merénylet napjához kötődik. Ez az esemény nemcsak a biztonság és szabadság alapkérdéseinek, hanem a kockázatelmélet, illetve a katasztrófavédelem elméleti alapjainak újragondolását is szükségessé tette.

Azzal, hogy a Világkereskedelmi Központ két tornyának egyszerre történő elpusztulását rendkívül kicsiny valószínűségére tekintettel elhanyagolták, és nem is kötöttek rá (együttes) biztosítást, a kockázatelemzésben új fejezet nyílt. A „nemvalószínűségi kockázat" fogalma eladdig nem létezett. Azon a napon azonban olyan esemény következett be, amelynek egyszerűen nem volt valószínűsége. Nem valószínűtlen volt, nem is zéróvalószínűségű, hanem *valószínűség nélküli*. Úgy valószínűség nélküli, ahogyan nincs értelme egy utcasarok népsűrűségéről beszélni, vagy ahogyan egy molekula hőmérséklete értelmezhetetlen.

Hibafa

A logikai kockázatelmélet alkalmazási területén található kockázati rendszerek állapotát úgynevezett hibafával lehet leírni, viselkedésüket pedig az úgynevezett hibafa-analízissel lehet elemezni (Henley-Kumamoto, 1981). A Wikipédia megfogalmazása szerint „A hibafa egy logikai diagram, ami egy rendszeren belül kimutatja egy lehetséges kritikus esemény és az azt elképzelhetően kiváltó okok között a kölcsönös kapcsolatot." A hibafa-módszer ma már csaknem félévszázados múltra tekint vissza. Elméletünk szűkebb, matematikai értelmében a hibafa használata a rendszert érő valamely nemkívánatos eseményt (pontosabban annak bekövetkezésére vonatkozó kijelentést, állítást) logikai műveletekkel visszavezeti bizonyos egyszerűbb, hatáskörünkben lévő úgynevezett primitív eseményekre. Tehát nem tárgyi

meghatározásra kell törekedni, hanem „explikatív" meghatározásra, más szóval logikai meghatározásra, a szükséges és elegendő feltételek megadására lásd (Russell, 1976).

Az, hogy egy kockázati rendszerre vonatkozóan mi minősül nemkívánatosnak, teljesen szubjektív megítélés kérdése, és az elmélet szempontjából érdektelen.[1] Igen gyakori, konfliktushelyzetekben pedig egyenesen tipikus, hogy ugyanaz az esemény egyidejűleg többféleképpen is megítélhető. Így például egy repülőgépnek egy felhőkarcolóval való ütközése egy terrorista számára lehet kívánatos, míg mások számára nem.

A hibafa-módszer mind hagyományos, mind pedig modernebb formájában hallgatólagosan feltételezi, hogy a vizsgálata tárgyát képező kockázati rendszer eseményei egy *rögzített logikai struktúrával* rendelkeznek. Más szóval feltételezi, hogy a kockázati rendszer környezetével való kapcsolata során megőrzi identitását, önazonosságát. Az elmélet alkalmazhatóságának ez szükséges, elengedhetetlen feltétele.

A legegyszerűbb közvetlen tapasztalatok mutatják, hogy a kockázati rendszerek önazonosságának megváltozása ma már szinte hétköznapi jelenség. Ha egy repülőgép (amelynek biztonsági kockázatát kitűnően le lehet írni és ki lehet számítani a hibafa-módszerrel, pontosabban: annak logikai kockázatelméleti modellje, az általunk használt szakkifejezéssel élve explikátuma alapján) összeütközik egy felhőkarcolóval (amelynek szintén jól ismert hibafája és így kockázati explikátuma van), akkor olyan új kockázati rendszerek állnak elő, amelyek többé nem kezelhetők az eredeti módszerrel. A repülőgéproncs jóllehet maga is kockázati rendszer, s mint ilyennek rendelkeznie kell valamilyen hibafával, ám viselkedése, állapotváltozásai, környezetével való kapcsolatai merőben más természetűek, mint bármelyik működő, bár mégoly veszélyes állapotú repülőgépé. Hasonló a helyzet a felhőkarcoló romjai vonatkozásában is. Sem a géproncs, sem a felhőkarcoló romjának hibafája nem vezethető le az eredetiekből, mert a kockázati rendszerek hibafája logikailag független a kölcsönhatásban nem lévő kockázati rendszerek hibafáitól.

Főesemény, csúcsesemény

A logikai kockázatelemzés tárgyát képező nemkívánatos eseménynek külön neve van: *csúcsesemény* (az angol „top event" tükörfordítása), illetve a magyarban emellett gyakran: *főesemény*. A főesemény az az esemény, amelyből a kockázatelemzés kiindul, ami a logikai kockázatelemzés közvetlen tárgya, amelynek szükséges és elegendő feltételeit keressük. A kockázatelemzés célja szükséges és elegendő feltételeket adni a főesemény bekövetkezésére. Az elemzés során nem valamely tényező számértéke, számszerű jellemzője (indikátora) az elemzés tárgya, illetve célja, hanem valamely jövőbeli lehetséges, vagy fiktív esemény bekövetkezésének szükséges és elegendő feltétele. A főeseményt mindig *negatív értelemben* célszerű megfogalmazni. Ez azt jelenti, hogy a logikai kockázatelemzési módszerrel nem azt vizsgáljuk, hogy miként *kell* valamely (kívánt) esemény (bekövetkezésé)t *elérni*, hanem azt, hogy miként *lehet* egy (nem kívánt) esemény (bekövetkezésé)t *elkerülni*. Ellentétben a nemkívánt eseménnyel, (amely a kockázatelmélet legfontosabb alapfogalma) a „kívánt esemény" nem tartozik a kockázatelmélet paradigmájához. A kívánt esemény semmiképpen sem interpretálandó úgy, mint a nemkívánt esemény ellentéte. Ugyanakkor magának a nemkívánatos eseménynek a jelentéstartalma *a módszer szempontjából* teljesen közömbös. A magyar szóhasználat annyiban szerencsés, hogy az angol „Top Event" (= „csúcsesemény") tükörfordítása mellett használja a „főesemény" szót. Annyiban azonban szerencsétlen, hogy a két fogalmat szinonim értelemben használja. Ennek oka az, hogy a kockázati rendszer

[1] Ugyanakkor a nemkívánatosnak minősülő esemény az alkalmazások gyakorlati szempontjából létfontosságú.

eseményeinek logikai viszonyait olyan fadiagrammal - a hibafával - ábrázolja, ami az úgynevezett „esemény*szintek”* tekintetében téves asszociációkat kelt.

Explikáció, explikátum, explikáns

A katasztrófák nemcsak földrajzi határokat nem ismernek, hanem diszciplináris korlátokat sem. Ez generálja egyfajta transzdiszciplinaritás parancsoló szükségszerűségét. Ennek két mélyenfekvő endogén oka van. Az egzakt tudományok sikereinek egyik alapvető záloga a módszeres *hanyagolás*, az *absztrakció*. Ugyanakkor a *lényegesnek* és a *létfontosságúnak* a radikális megkülönböztetése. Az elméleti mechanika (egyik részdiszciplínája) a súrlódást elhanyagolja. Ha egy (nem megfelelően síkosság-mentesített) úttesten életveszélyes baleset történik, azt a mechanika fogalmi rendszerében meg sem lehet fogalmazni. A tudományos diszciplínák külön-külön azért képtelenek a katasztrófajelenség elméleti kezelésére (adekvát leírására, értelmezésére, megelőzésére, előrejelzésére), mert paradigmájukban pontosan azokat a tényezőket hanyagolják el, amelyek a katasztrófák létrejöttében létfontosságúak. Ellentétben tehát az egzakt tudományokkal, a katasztrófák elméletében *minden, ami létfontosságú, az lényeges is*. Ez azonban nem jelenti azt, hogy a katasztrófák elmélete nem lehet egzakt tudomány. Csak annyit jelent, hogy figyelembe kell vennie mindazt, ami a szaktudományok paradigmájában közös.

A jelen tanulmány azt a módszert állítja előtérbe, amely ezt a célt szolgálja. E módszer neve: *explikáció*[2]. Intuitíve annyit jelent, mint a jelenségek leírásában a közvetlen logikai megfogalmazást alkalmazni szemben a *definitív* leírásmóddal.

A katasztrófák elméletében arra a kérdésre keressük a választ, hogy az egymást követő, egymásra épülő sorozatos fogalmi részletezéssel, szükséges és elegendő feltételeket keresünk mindaddig, amíg - valamely adott helyzetben - saját hatáskörünkben operacionalizálható eseményekhez és információkhoz nem jutunk. Ez az explikáció intuitív tartalma.

Most már egzakt módon megfogalmazva: azt az eljárást, amelyben az elemzés során adódó eseményekre vonatkozó állításokhoz ismételten szükséges és elegendő feltételeket adunk meg, alapvető fontossága okán külön névvel *explikációnak* nevezzük (a latin „explicare” = „kifejteni”, „explicitté tenni” alapján). Ebben a terminológiában tehát a kockázatelemzés lényegileg explikáció. Ebben a kontextusban a fogalom már a hazai szakirodalomban is alkalmazásra került. (Lásd (Bukovics-Molnár, 2000)).

Valamely esemény *összes kiváltó* tényezőjének megállapítását az esemény *diszjunktív explikációjának* nevezzük. Itt az „összes” szigorúan technikai értelemben értendő. Azt jelenti, hogy ezek *bármelyike* (bekövetkezése) kiváltja, előidézi, maga után vonja a szóban forgó eseményt (bekövetkezését), a többi esemény bekövetkezésétől függetlenül. A diszjunktív explikáció eredményeként előálló esemény neve: az esemény *diszjunktív explikátuma*. A kiváltó tényezők ennek *tagjai*, illetve *explikánsai*.

Valamely esemény *összes akadályozó* tényezőjének megállapítását az esemény *konjunktív explikációjának* nevezzük. Itt is az „összes” szigorúan technikai értelemben értendő. Azt jelenti, hogy ezek bármelyike (be nem következése) megszünteti, megelőzi, elhárítja, megakadályozza a szóban forgó esemény (bekövetkezését)t, a többi eseménytől függetlenül. A konjunktív explikáció eredményeként előálló esemény neve: az esemény konjunktív explikátuma, az akadályozó tényezők ennek *tényezői*, illetve *konjunktív explikánsai*.

A logikai kockázatelmélet a vizsgálatának tárgyát képező kockázati rendszer explikátumát adottnak veszi. [3]

---

[2] Az explikáció fogalmának kifejtésére nézve Lsd. (Carnap, 1950.)

[3] A kockázati rendszerek explikátumának fogalma centrális jelentőségű az elméletben.

Kiváltás, hárítás

Az elemzés során meg kell határozni (szükség esetén szakértői team-munkával) a főesemény összes *szinguláris* kiváltó, vagy *szinguláris* akadályozó tényezőjét. Valamely esemény szinguláris kiváltó tényezőjén olyan esemény értendő, amelyre igaz, hogy az esemény mindannyiszor bekövetkezik, valahányszor *legalább egy* kiváltó tényezője (más szóval aktiváló tényezője) bekövetkezik. A *szinguláris akadályozó tényező* hasonlóan értendő.

Iteráció

A logikai kockázatelemzés során nemcsak a főesemény, hanem annak (diszjunktív, illetve konjunktív) explikátuma explikációját is el kell végezni. Az explikációs eljárást az explikátumokra ismételni kell mindaddig, amíg az alábbi okok egyike fenn nem áll. Ezt az eljárást *iterácónak*, részletesebben *iteratív explikációnak* nevezzük.

- Olyan taghoz vagy tényezőhöz érkeztünk, amelynek bekövetkezése, vagy elmaradása „kézben tartható", „hatáskörünkben van", azaz valamely személy, vagy intézmény egyetlen elemi aktusával hatáskörében biztosítható, illetve megítélhető;
- Olyan taghoz, vagy tényezőhöz érkeztünk, amelynek további explikációját a körülmények (tárgyi vagy személyi feltételek hiánya, időkorlátok, stb.) nem teszik lehetővé;
- Olyan taghoz vagy tényezőhöz érkeztünk, amelynek hatását a már felsorolt események (együttesen, vagy külön-külön) kompenzálhatják, helyettesíthetik fedhetik, kiválthatják, vagy kiküszöbölhetik.

Primitív események

A jelen tanulmány kontextusában az explikáció pontosabban annyit jelent, mint (1) megállapítani valamely esemény bekövetkezésének szükséges és elegendő feltételét. Ennek eredménye az esemény explikátuma (2), megállapítani minden explikátum explikátumát, hacsak ennek valamely akadálya fel nem merül. Így előállnak explikálatlan explikátumok. Ezeket *primitív eseményeknek* vagy röviden *prímeseményeknek* nevezzük.

Egyszerűen kifejezve, a prímesemények olyan események, amelyeket az adott eseményrendszerben nem lehet visszavezetni más eseményekre, őket nem indukálja más esemény, ők azonban más eseményeket indukálnak, és minden esemény logikailag rájuk vezethető vissza.

A prímesemények köre értelemszerűen megegyezik az általunk kézben tartott események körével, hiszen nem függnek rajtunk kívül álló tényezőktől.

Az ókori bölcs (Epiktétosz, 2001) briliáns esszében-tanításban fejti ki voltaképpen a *prímesemény* (ha tetszik az alapesemény, a „gyökér-ok" stb.) fogalmát. Alapaxiómája: „Bizonyos dolgok hatalmunkban vannak, más dolgok nincsenek" Következtetései ma figyelemreméltóbbak, mint valaha.

Szaknyilatkozat, rendszámok

Az explikáció befejeztével előáll az explikátumok egy összessége. Az ebből létrehozott, bizonyos formai követelményeknek eleget tevő explikációs lista neve: *szaknyilatkozat*. Ezt más néven a kockázati rendszer (főeseményével megnevezett) *explikátumának* is nevezzük. A szóbanforgó kockázati rendszert esetenként az *explikált kockázati rendszer* elnevezéssel illetjük. A szaknyilatkozat legfőbb formai sajátossága, hogy szisztematikusan feltünteti az

explikáció során előálló alá- és fölérendelési viszonyokat, valamint az explikánsok logikai *típusá*t. Az előbbi a *rendszámok* alkalmazásában jut kifejezésre. A rendszám alkalmazásával bármely két explikánsról *pusztán rendszámaik alapján* egyértelműen meghatározható a közöttük lévő *hierarchikus logikai viszony*, vagyis az, hogy az egyik *implikálja*-e a másikat, illetve, hogy milyen *explikációs útvonalon* érhető el egyik a másikból.

A "*Rendszámintegritás*" azt jelenti, hogy egy esemény explikánsainak rendszáma nem hagyhat ki értékeket: utolsó jegyeinek mindig eggyel kell növekedniök az explikánsok sorrendjében.

Konjunktív és diszjunktív normálforma

A *konjunktív normálforma* a prímesemények és a főesemény bekövetkezése közötti logikai kapcsolatrendszer olyan megjelenítési formája, ahol a főesemény állapotát úgy vezetjük vissza prímesemények csoportjainak állapotára, hogy ha mindegyik itt szereplő csoportban a csoporthoz tartozó akár csak egyetlen prímesemény aktív, akkor a főesemény is aktív. (Ezeket a csoportokat erős pontoknak nevezzük.)

A *diszjunktív normálforma* a prímesemények és a főesemény bekövetkezése közötti logikai kapcsolatrendszer olyan megjelenítési formája, ahol a főesemény állapotát úgy vezetjük vissza prímesemények csoportjainak állapotára, hogy ha akár csak egyetlen itt szereplő csoportban a csoporthoz tartozó minden egyes prímesemény aktív, akkor a főesemény is aktív. (Ezeket a csoportokat gyenge pontnak nevezzük.)

A normálformák szabatos matematikai tárgyalása megtalálható a matematikai logikai szakirodalomban. (Lsd. (Demetrovics, 1985), (Birkhoff – Bartee, 1974), (Jaglom, 1983)).

Erős és gyenge pontok

Erős pont a prímesemények és a főesemény bekövetkezése közti logikai kapcsolatrendszer konjunktív normálformájának egyik prímesemény-csoportja, ahol az összes ilyen csoport bármelyik komponensének aktív állapota a főesemény aktív állapotát idézi elő.

Gyenge pont a prímesemények és a főesemény bekövetkezése közti logikai kapcsolatrendszer diszjunktív normálformájának egyik prímesemény-csoportja, ahol a csoport minden komponensének egyidejű aktív állapota a főesemény aktív állapotát idézi elő.

A logikai hadviselés fogalma

A fentiek alapján most már visszatérhetünk a logikai hadviselés fogalmára. A normálformák, valamint az erős és gyenge pontok ismeretében meg tudjuk mondani, mely prímesemények passziválása vezet az aktív főesemény passziválásához, illetve mely prímesemények aktiválása vezet a passzív főesemény aktiválásához.

Főeseménynek az általunk elérni vagy éppen elkerülni kívánt eseményt tekintjük, és így meg tudjuk mondani, hogy a prímesemények közül – amelyek köre, mint láttuk, megegyezik az általunk kézben tartott események körével – pontosan melyek biztosítják a főesemény számunkra kívánatos állapotát.

Így tehát nem kell időt, pénzt, energiát, esetleg emberéletet pazarolnunk olyan prímesemények aktiválására vagy passziválására, amelyeknek valójában nincs hatásuk eredeti célunk elérésére. Ez a logikai hadviselés általunk használt fogalma.

PÉLDA: SIKERES MERÉNYLET

A "sikeres merénylet" kifejezés - a jelen szövegösszefüggésben - csupán egy rövidítés és azt a kijelentést helyettesíti, hogy "Adott helyen és időben történő sikeres merénylet kockázatának mértéke megengedhetetlenül nagy".

Itt tehát az a nemkívánatos esemény, hogy sikeres a merénylet. A sikeres (értsd: a merénylő szempontjából sikeres) merénylet kockázatelemzését a merényletvédelemnek kell elvégeznie. A sikertelen merényletnek általános esetben a sikeres merényletétől részben vegy egészben különböző kockázati tényezői lehetnek.

Ez az a kijelentés, amit sorozatos ismétléssel (szukcesszív approximációval) egyre elemibb (azaz egyre könnyebben eldönthető) kijelentésekre bontunk a szaknyilatkozat összeállítása során.

Először szöveges formában fogalmazzuk meg a hibafát. Ez nem egyéb, mint a szaknyilatkozat.

A következő tény:

SIKERES MERÉNYLET

(mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek mindegyike (mint nemkívánatos körülmény) fennáll:

- (1) INDÍTÉK,
- (2) CÉLSZEMÉLYEK,
- (3) CÉLTÁRGYAK,
- (4) IDŐZÍTÉS,
- (5) HELYSZÍN,
- (6) KIVITELEZÉS.

1 INDÍTÉK

(mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:

- (1.1) ANYAGI INDÍTÉK, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
  - (1.1.1) PÉNZKÖVETELÉSSEL,
  - (1.1.2) TÁRGYKÖVETELÉSSEL.
- (1.2) VALLÁSI INDÍTÉK,
- (1.3) POLITIKAI INDÍTÉK,
- (1.4) SZEMÉLYES INDÍTÉK,
- (1.5) ETNIKAI INDÍTÉK.

2 CÉLSZEMÉLYEK

(mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:

- (2.1) MAGÁNSZEMÉLYEK,
- (2.2) KÖZSZEREPLŐK.

3 CÉLTÁRGYAK

(mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:

- (3.1) ÉPÜLET, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
    - (3.1.1) ÉPÜLET KIFOGÁSOLHATÓ KIALAKÍTÁSA,
    - (3.1.2) ÉPÜLET KIFOGÁSOLHATÓ FELÜGYELETI RENDSZERE.
- (3.2) JÁRMŰ, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
    - (3.2.1) JÁRMŰ KIFOGÁSOLHATÓ KIALAKÍTÁSA,
    - (3.2.2) JÁRMŰ KIFOGÁSOLHATÓ FELÜGYELETI RENDSZERE.

4 IDŐZÍTÉS

(mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:

- (4.1) ELLENŐRZÉSMULASZTÁSSAL, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
    - (4.1.1) TŰZVÉDELMI ELLENŐRZÉS MULASZTÁS, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
        - (4.1.1.1) FELTÁRT HIÁNYOSSÁG MEGSZÜNTETÉS MULASZTÁS,
        - (4.1.1.2) FELTÁRT HIÁNYOSSÁG KOMMUNIKÁCIÓS MULASZTÁS,
        - (4.1.1.3) EGYÉB TŰZVÉDELMI ELLENŐRZÉS MULASZTÁS.
    - (4.1.2) VEGYVÉDELMI ELLENŐRZÉS MULASZTÁS ,
    - (4.1.3) BELÉPTETÉSI ELLENŐRZÉS MULASZTÁS.
- (4.2) ELLENŐRZÉSKIJÁTSZÁSSAL,
- (4.3) ERŐSZAKKAL,
- (4.4) FIGYELMEZTETÉSSEL.

5 HELYSZÍN

(mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:

- (5.1) KÖZTERÜLET, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
    - (5.1.1) KÖZTERÜLET KIFOGÁSOLHATÓ KIALAKÍTÁSA,
    - (5.1.2) RENDŐRI JELENLÉT HIÁNYA KÖZTERÜETEN,
    - (5.1.3) KIFOGÁSOLHATÓ KÖZTERÜLETI TITKOS ÜGYKEZELÉS.
- (5.2) MAGÁNTERÜLET, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
    - (5.2.1) MAGÁNTERÜLET KIFOGÁSOLHATÓ KIALAKÍTÁSA,
    - (5.2.2) RENDŐRI JELENLÉT HIÁNYA MAGÁNTERÜLETEN,
    - (5.2.3) KIFOGÁSOLHATÓ MAGÁNTERÜLETI TITKOS ÜGYKEZELÉS.

- (5.3) NEMZETKÖZI TERÜLET, (mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:
    - (5.3.1) NEMZETKÖZI TERÜLET KIFOGÁSOLHATÓ KIALAKÍTÁSA,
    - (5.3.2) RENDŐRI JELENLÉT HIÁNYA NEMZETKÖZI TERÜLETEN,
    - (5.3.3) KIFOGÁSOLHATÓ NEMZETKÖZI TERÜLETI TITKOS ÜGYKEZELÉS.

6 KIVITELEZÉS

(mint nemkívánatos esemény) esete akkor és csak akkor áll fenn, ha az alábbi feltételek egyike (mint nemkívánatos körülmény) fennáll:

- (6.1) TÚSZEJTÉS,
- (6.2) ROBBANTÁS,
- (6.3) LŐFEGYVER,
- (6.4) ÖNGYILKOS.

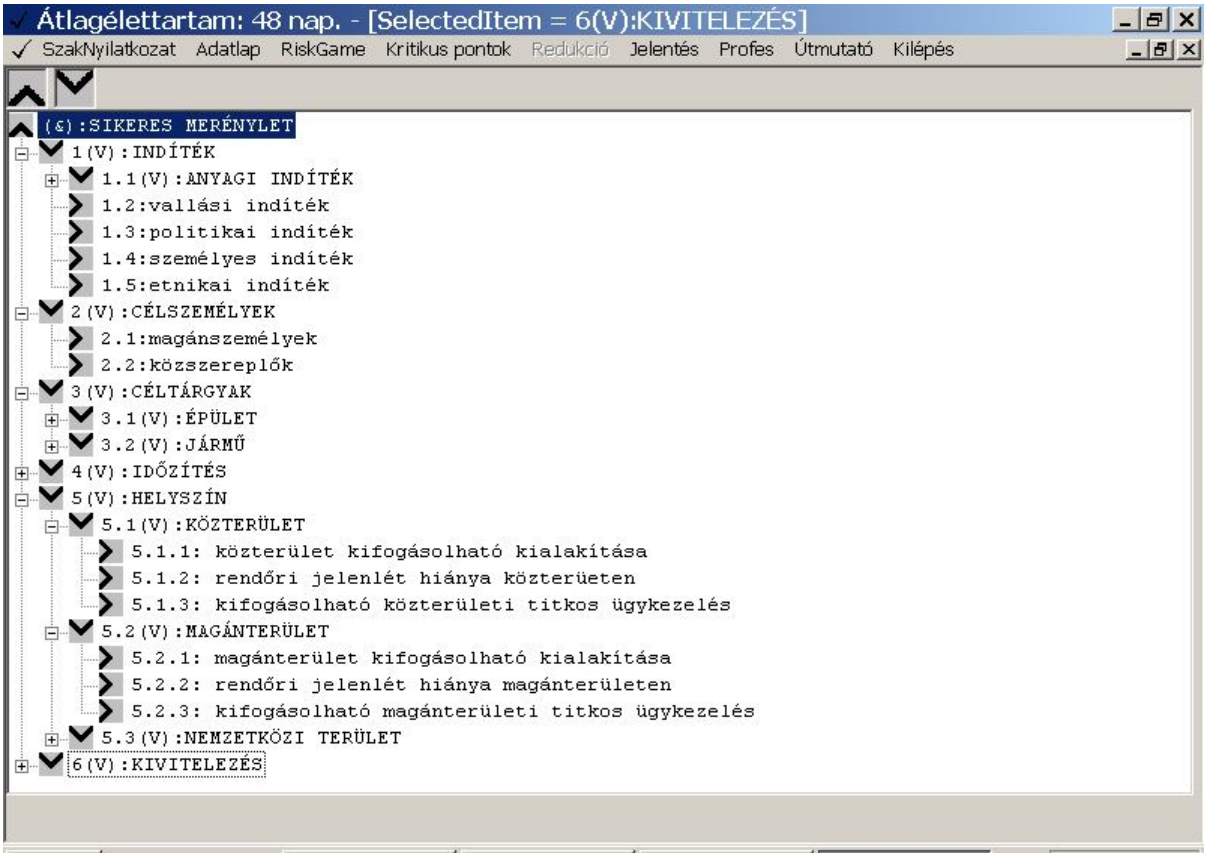
A fentieket a Profes+4 szoftver képernyőképeivel illusztráljuk. (A szoftver a PROFES Környezetbiztonsági Programiroda Kft, http://www.profes.hu terméke.) Először a majdnem teljesen összecsukott hibafát látjuk.

A hibafa jelölései:

- Az **Λ** szimbólum a főesemény sorát jelöli. (Szóban „és”-nek illetve „et”-nek szokás ejteni.)
- A **V** szimbólum egy explikálható esemény sorát jelöli, és explikánsai a következő sorokban találhatók. Szóbeli ejtése: „vagy”, a szó megengedő értelmében, tehát mint „legalább az egyik”. Ez nem tévesztendő össze a mindennapi nyelvben használt „kizáró vagy”-gyal, amit a „vagy-vagy” fejez ki.
- A **>** szimbólum egy prímesemény sorát jelöli. (Szóbeli ejtésére nincsen kialakult szokás.)
- Az (&) („et”) szimbólum (csakúgy, mint az **Λ**) arra utal, hogy az adott sorban található esemény közvetlen explikánsai között az explikációban konjunkciós kapcsolat áll fenn.
- A (V) szimbólum arra utal, hogy az adott sorban található esemény közvetlen explikánsai között az explikációban diszjunkciós kapcsolat áll fenn.
- Az **Λ**, **V** és **>** szimbólumok mögötti, többnyire pontokkal tagolt számok az események *rendszámai.* Ezek (az események jelentésétől függetlenül) megmutatják, hogy melyik esemény melyiknek a következménye. Ennek akkor van jelentősége, amikor a kockázatelemzőnek titkos anyagból kell dolgoznia.
- A logikai kockázatelemzés során a szaknyilatkozatból levont minden következtetés a logikai törvényei alapján bizonyíthatók és érvényük független a szóbanforgó események jelentésétől

1. ábra. A Profes+4 program képernyője összecsukott hibafával

A következő ábrán a majdnem teljesen kinyitott hibafát látjuk (azért csak majdnem teljesen, mert a teljes hibafa nem fér rá a képernyőre).



2. ábra. A Profes+4 program képernyője majdnem teljesen kinyitott hibafával

A következő táblázat a prímesemények különböző azonosítóit tartalmazza. Az eseménykód a rendszámot jelenti.

SOR	ESEMÉNYKÓD	ESEMÉNYNÉV
01	1.2	vallási indíték
02	4.2	ellenőrzéskijátszással
03	2.1	magánszemélyek
04	2.2	közszereplők
05	6.1	túszejtés
06	6.2	robbantás
07	6.3	lőfegyver
08	1.3	politikai indíték

SOR	ESEMÉNYKÓD	ESEMÉNYNÉV
09	1.4	személyes indíték
10	6.4	öngyilkos
11	4.3	erőszakkal
12	4.4	figyelmeztetéssel
13	1.5	etnikai indíték
14	5.1.1	közterület kifogásolható kialakítása
15	5.1.2	rendőri jelenlét hiánya közterületen
16	5.2.1	magánterület kifogásolható kialakítása
17	5.2.2	rendőri jelenlét hiánya magánterületen
18	5.3.1	nemzetközi terület kifogásolható kialakítása
19	5.3.2	rendőri jelenlét hiánya nemzetközi területen
20	5.1.3	kifogásolható közterületi titkos ügykezelés
21	5.2.3	kifogásolható magánterületi titkos ügykezelés
22	5.3.3	kifogásolható nemzetközi területi titkos ügykezelés
23	3.1.1	épület kifogásolható kialakítása
24	3.1.2	épület kifogásolható felügyeleti rendszere
25	3.2.1	jármű kifogásolható kialakítása
26	3.2.2	jármű kifogásolható felügyeleti rendszere
27	1.1.1	pénzköveteléssel
28	1.1.2	tárgyköveteléssel
29	4.1.2	vegyvédelmi ellenőrzés mulasztás
30	4.1.3	beléptetési ellenőrzés mulasztás
31	4.1.1.1	feltárt hiányosság megszüntetés mulasztás
32	4.1.1.2	feltárt hiányosság kommunikációs mulasztás
33	4.1.1.3	egyéb tűzvédelmi ellenőrzés mulasztás

1. táblázat. A „Sikeres merénylet” főesemény primitív eseményeinek azonosítói

Most nézzük a kritikus pontokat. Ezeket ugyancsak a Profes+4 szoftver számította ki. A műveleti jelek közül, szokásos módon, „+” a „logikai vagy” (diszjunkció), „x” pedig a „logikai és” (konjunkció) jele.

Először a konjunktív normálformából származtatott erős pontokat soroljuk fel.

3+4

5+6+7+10

23+24+25+26

1+8+9+13+27+28

2+11+12+29+30+31+32+33

14+15+16+17+18+19+20+21+22

Ezután a diszjunktív normálformából származtatott gyenge pontokat soroljuk fel, de csak részben, mert számuk több ezer.

1x3x5x14x25x31

1x4x5x14x23x31

3x5x14x23x27x30

3x6x14x23x27x31

3x7x14x23x27x31

3x10x14x23x27x31

3x5x14x23x27x32

3x5x14x23x27x33

4x7x22x26x28x32

4x7x22x26x28x33

4x10x19x26x28x32

4x10x19x26x28x33

4x10x22x26x28x32

4x10x22x26x28x33

Mint látjuk, a 3. és 4. prímesemények együttes passziválása passzivál egy erős pontot, egyúttal pedig természetesen a főeseményt is passziválja.

Ugyancsak látható, hogy a felsorolt 14 gyenge pontot passziválhatjuk az előbb említett két prímesemény, a 3. és 4. passziválásával. Ez igaz a többi, itt fel nem sorolt gyenge pontra is, így tehát a főeseményre is. Vagyis a gyenge pontok nagy száma egyáltalán nem jelent kezelhetetlenséget.

Ha azonban tartalmilag is megnézzük, mit jelent ez a két prímesemény, azt látjuk, hogy a célszemélyek közül a közszereplők és a magánszemélyek elleni merényletet. Mivel ez a két csoport nyilvánvalóan minden, elvileg egyáltalán szóba kerülő személyt tartalmaz, ezért a két csoport elleni merénylet kizárásának szükségessége trivialitás.

Nézzük tovább a konjunktív normálformát (azért azt, mert jelen esetben áttekinthetőbb a diszjunktív normálformánál). Látjuk, hogy az 5., 6., 7. és 10. prímesemények egyidejű passziválása ugyamcsak passziválja a főeseményt. Tartalmilag azonban megint trivialitást kapunk, hiszen az említett 4 prímesemény lefedi az elvileg szóba kerülő összes elkövetési módot.

Tovább keresve, a 23., 24, 25., 26. prímesemény-csoportot találjuk erős pontként. Itt az épület és/vagy jármű kifogásolható kialakításáról és/vagy felügyeleti rendszeréről van szó, ezeknek a veszélyforrásoknak a passziválása viszont már nem trivialitásként vezet a sikeres merénylet passzíiv állapotban tartásához. Ugyanez látszik a gyenge pontok alapján is, hiszen az említett prímesemény-csoport valamelyik tagja mindegyik gyenge pontban megtalálható.

A KORSZERŰ HADVISELÉSI ELVEK KAPCSOLATA

Korábban már láttuk, hogyan fejlődött ki a platform-alapú hadviselésből kiindulva a hálózat-alapú és az entrópia-alapú hadviselés. Nézzük most meg ezek tartalmi kapcsolatait.

A hálózat-alapú hadviselés abban különbözik a platform-alapútól, hogy a saját és az ellenséges erőket egyaránt hálózatukkal együtt, azzal összefüggésben szemléli, és figyelembe veszi a hálózat nyújtotta lehetőségeket. Nincs azonban különbség abban a tekintetben, hogy mindkét hadviselési elv az anyagi eszközök struktúrájával foglalkozik, elsődlegesen azt kívánja rombolni, és a rombolás valószínű, de bizonytalan következményeként várja az ellenség harcképességének csökkenését.

Az entrópia-alapú hadviselésben viszont nem a rombolás az elsődleges, hanem az ellenség zavarodottságának előidézése. Ehhez az ellenség hálózatának működését kívánja oly mértékig akadályozni, gátolni, hogy az ellenség képtelen legyen szervezett, rendezett cselekvésre.

A platform-alapú, a hálózat-alapú és az entrópia-alapú hadviselésben közös, hogy mindegyikük a fizikai struktúrára (ideértve az informatikát is) koncentrál. A történelmi tapasztalatok azonban azt mutatják, hogy ez a megközelítés nem mindig hatékony, különösen nem az a korunkra jellemző aszimmetrikus háborús szituációkban. Ha az ellenség infrastruktúrája kezdetleges, annak lerombolása nem csökkenti lényegesen az ellenfél harcképességét, mert az ilyen infrastruktúra könnyen helyreállítható.

A LOGIKAI HADVISELÉS SZEMLÉLETE

A logikai hadviselés koncepciója új megközelítést ajánl. Az alapcél az ellenség hálózatának megbénítása illetve összezavarása változatlan, de megvalósítását nem a hálózat elleni közvetlen támadás bizonytalan következményeként várjuk. Nem a struktúrát támadjuk, hanem a funkciót. Az elvnek megfelelő eljárás a következő lehet:

Hálózat-alapú hadviselés esetén alapcél az ellenség hálózatának megbénítása (ennek pedig csak esetleges kivitelezési módja a fizikai rombolás).

(1) Az erős és gyenge pontok ismeretében úgy választjuk meg az aktiválandó vagy passziválandó prímesemények csoportját, hogy lehetőleg ne lépjünk túl a kívánatos cél elérését biztosító minimális beavatkozáson (romboláson).

(2) Visszakeressük a hibafában, mely összetett eseményben vagy eseménykombinációban találkoznak a kiválasztott prímesemények.

(3) A hibafából visszakövetkeztetünk arra, hogy a fizikai rendszerben melyik az a pont, amelynek megtámadása a (2)-ben azonosított eseménykombinációnak felel meg.

Entrópia-alapú hadviselés esetén az alapcél az ellenség entrópiájának növelése (és ennek ismét csak esetleges eszköze lehet a fizikai rombolás). Olyan hibafa esetében, amelyben túlnyomó a diszjunktív elágazások aránya, a működés átlátható, a rendszert nehéz megzavarni, hiszen ritkán kell több feltételnek egyszerre teljesülni a normális működéshez. Ezért az entrópia növelésének éppen a hibafa konjunktív elágazásai számának növelése az eszköze. Vagyis el kell érni az ellenség struktúrájának módosítását, hogy ezáltal a hibafa is módosuljon. Ezt például – elméletileg – oly módon lehet elérni, hogy kiiktatjuk az ellenség rendszerének egy olyan komponensét, amelyet csak konjunktívan kapcsolt elemek csoportjával lehet pótolni.

(1) Az erős és gyenge pontok ismeretében megnézzük, milyen prímesemény-csoportok aktiválása vagy passziválása okoz pótlandó veszteséget az ellenségnek.

(2) Úgy választjuk meg az aktiválandó vagy passziválandó prímesemények csoportját, hogy rákényszerítsük az ellenséget arra, hibafáját konjunktív elágazásokkal egészítse ki.

(3) A hibafából visszakövetkeztetünk arra, hogy a fizikai rendszerben hol van az a pont, amelynek megtámadása a (2)-ben azonosított eseménykombinációnak felel meg. Például egy szállítási vagy kommunikációs vonal lezárásával elérhetjük, hogy ezt több más vonal konjunktív összekapcsolásával pótolja.

Az eljárást ismételve fokozatosan növelhető az ellenség entrópiaszintje, és egy idő után eléri az ellenállásképtelenség mértékét.

Láthatjuk, hogy a logikai hadviselés lehetővé teszi célunk elérését a feltétlenül szükségesnél nem több prímesemény felhasználásával, vagyis a feltétlenül szükségesnél nem nagyobb erőfeszítés és rombolás alkalmazásával.

KITEKINTÉS

Az előbbiekben vázolt entrópia alapú koncepció pontos matematikai megfogalmazása jogos elvárás, mert az entrópia jól ismert mennyiség, matematikai tulajdonságai tisztázottak. Ez azért is fontos lenne, mert az entrópia-alapú hadviselésben központi szerepet játszó entrópianövelés számszerűsítése lehetővé tenné, hogy az ellenség számára pontosan „adagoljuk” a harcképességet bénító stresszt.

Felhasznált irodalom

[1] Alberts, D.S., Garstka, J.J., Stein, F.P., (2000) Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP Publ., 2nd Edition (Revised). Aug 1999.

[2] Arquilla, J. – Ronfeldt, D.F. (1995): Information, Power, and Grand Strategy (unpublished) Santa Monica: The RAND Corporation, July 1995, p. 19.

[3] Birkhoff, G. –Bartee, T.C. (1974): A modern algebra a számítógéptudományban. Műszaki Könyvkiadó, Budapest, 1974.

[4] Bukovics István – Molnár Gábor (2000): Munkahelyi tűzvédelem. Verlag Dashöfer Szakkiadó, Budapest (2000)

[5] Cebrowski, VAdm Arthur K., USN, and John J. Garstka (1998): "Network Centric Warfare: Its Origin and Future." Proceedings of the Naval Institute 124:1 (January 1998): 28–35.

[6] Demetrovics János – Jordan Denev – Radislav Pavlov (1985): A számítástudomány matematikai alapjai. Tankönyvkiadó, Budapest, 1985.

[7] Dunn III, Charles. Powell, Gregg. Martin, Christopher. Hamilton, Michael. Pangle II, Charles (2004): "Information Superiority/Battle Command (Network Centric Warfare Environment)", Command and Control Research Technology Symposium, San Diego, 2004.

[8] Epiktétos (2001): Epiktétos kézikönyvecskéje, vagyis a stoikus bölcs breviáriuma. Gladiátor Könyvkiadó, Budapest, 2001.

[9] Henley, E.J. – Kumamoto, H. (1981): Reliability Engineering and Risk Assessment. Prentice Hall, 1981.

[10] Herman, Mark (1997): Entropy-based warfare: A unified theory for modeling the Revolution in Military Affairs, Booze, Allen and Hamilton Inc, 1997.

[11] Jaglom, I.M. (1983): Boole struktúrák és modelljeik. Műszaki Könyvkiadó, Budapest, 1983.

[12] Johnson, Adm Jay L., USN (1997): Address at the U.S. Naval Institute Annapolis Seminar and 123d Annual Meeting, Annapolis, MD, 23 April 1997.

[13] Quine, Willard Van Orman (1968): A logika módszerei. Akadémiai Kiadó, Budapest, 1968.

[14] Russell, Bertrand (1976): Miszticizmus és logika. Magyar Helikon, Budapest, 1976.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Muha Lajos – Tóth Georgina Nóra
muha.lajos@zmne.hu - toth.georgina@bgk.uni-obuda.hu

A BANKBIZTONSÁG VIZSGÁLATA KOCKÁZATELEMZÉSSEL

Absztrakt

Minden szervezet esetében a biztonság a stratégiai célokat szolgálja. Különösen igaz ez a piaci körülmények között működő társaságoknál, ahol a biztonság a védendő értékek megőrzésén túlmenően, a működés folyamatosságában is fontos szerepet játszik. A biztonság megteremtése szempontjából elengedhetetlen egy hatékony kockázatelemzés elvégzése. Jelen cikkben pénzintézetek esetén jól alkalmazható biztonsági vizsgálatának előkészítésével és folyamatával foglalkozunk. Ennek során egy hatékony kockázatelemzési módszertant dolgoztunk ki.

For most institutions security is part of their strategy. This is especially true for profit-oriented institutions, where security not only protects their investments but also ensures continuous revenue to continue their operation. For these institutions it is essential to carry out a detailed risk assessment analysis in order to ensure security. In this paper we investigate the preparation and procedure of security evaluation for monetary institutions. For this, we prepared an effective methodology for risk assessment analysis.

Kulcsszavak: *bankbiztonság, biztonsági vizsgálat, kockázatelemzés ~bank security, security audit, risk analysis*

BEVEZETÉS

A pénzintézetek esetében – alapfunkcióikból eredően – az általuk őrzött és kezelt alapértékek, a fizető eszközök, az értékpapírok közvetett és közvetlen biztonságának garantálása alapvető érdekük, mert az ezen értékek elleni sikeres támadások nemcsak közvetlenül számszerűsíthető károkat, hanem komoly presztízsveszteséget is okozhatnak. Ez utóbbi pedig vevői bizalomvesztés előidézésén keresztül további károkat is okozhatnak.

Ezen túlmenően az olyan fenyegetések, amelyek a pénzintézet működésének folyamatosságát, az általuk kezelt érzékeny információk, adatok bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztetik, szintén komoly veszélyt jelentenek a profittermelő képességre.

A fentiekből következik, hogy az *értékmegőrzés*, a *forgalom és működés folyamatosságának biztosítása*, valamint az informatikai biztonság megőrzése azok a kiemelten fontos védelmi célok, amelyek a komplex védelem kialakításánál meghatározóak. A szervezet védelmi céljain túlmenően, a védelmi intézkedéseknek a jogszabályokban, a pénzintézetekre vonatkozó előírásokban és ajánlásokban megfogalmazott biztonsági előírásoknak is meg kell felelni. A pénzintézet belső biztonsági előírásaival együtt ezek egy olyan szabályozási követelményrendszert adnak, amelyek meghatározóan hatnak az adminisztratív védelmi rendszerre és szintén a korábban megfogalmazott védelmi célokat szolgálják.

A biztonság megteremtése és fenntartása szempontjából elengedhetetlen egy hatékony kockázatelemzés elvégzése. Ehhez valamilyen kockázatelemzési módszertant kell felhasználni. Számos kvalitatív és kvantitatív kockázatelemzési módszertan létezik, ezek közül széles körben ismert:

- az informatikai biztonsági kockázatok elemzésére használt CRAMM (Central Computer and Telecommunications Agency: Risk Analysis and Management Method) [1],
- az ipari veszélyek és működési problémák feltárására használt HAZOP (Hazard and Operability Studies) [*2*],
- a deduktív hibaanalízisre használt FTA (Fault Tree Analysis) [3],
- a hibaforrások azonosítására használt FMEA (Failure Modes and Effects Analysis) [4],

Ebben a munkában a brit kormány Központi Számítógép és Távközlési Ügynökség, a CCTA által kidolgozott CRAMM kvalitatív kockázatelemzési és kezelési módszertanát használtuk fel, mivel ez, ha nem is a bankbiztonsági kockázatok, de biztonsági kockázatok elemzésére készült, és arra számos alkalommal felhasználásra került hazánkban is. A választás mellett szólt, hogy az ezen a módszertanon alapuló szoftvereszközt alkalmaz a NATO. Ez a módszertan került feldolgozásra például a Közigazgatási Informatikai Bizottság 25. számú ajánlásának a biztonsági vizsgálatokkal foglalkozó kötetében [5] is.

VÉDELMI CÉLOK

A pénzintézetek esetében a következő védelmi célok meghatározóak a kockázatelemzésben:

- Minden védendő alapértékre (fizető eszközök, értékpapírok) és az azokat körülvevő rendszerelemekre (épület, infrastruktúra, személyzet, stb.) meghatározandók a releváns fenyegetések és a védelmek gyenge pontjai, amelyek ismeretében olyan intézkedési javaslatok alakíthatók ki, amelyekkel javítani lehet a védelem teljes körűségét és zártságát.

- A védelemi képességeknek időben folyamatosan biztosítottaknak kell lenniük. Az egyszer már kellő szinten megvalósított védelmi képességek erodálása (fegyelmezetlenség, hanyagság, a biztonság fontosságának nem kellő tudatosítása miatt, a technika szinten tartásának hiánya és erkölcsi elavulása) is veszélyezteti a folyamatosságot. Ennek fenntartásában fontos szerepet játszik a szabályozottság kielégítő szintje, annak betartása és betartatása. Fontos a folyamatosság biztosításának és biztosítottságának, a szabályozottság, a jogszabályi megfelelősség és ezek ellenőrzésének meghatározott időközönkénti vizsgálata.
- A zárt, teljes körű és folytonos védelem önmagában még nem biztosítja a védelmi képességek a szervezet elfogadható mértékét. Ehhez elengedhetetlen a kockázatok ismerete, de legalábbis közelítő szintű becslése. A kockázatok felmérése, elemzése és minősítése, abból a célból történik, hogy a védelmi rendszerek tervezése, továbbfejlesztése során olyan védelem kerüljön kialakítása, amely a rendszer minden pontján kockázatokkal arányos védelmet nyújt úgy, hogy közben figyelembe veszi a védelem kiépítésének és üzemeltetésének költségeit.

A bankbiztonsági vizsgálat igen sokrétű. Holisztikus megközelítésben ki kell térnie a pénzintézet működésre és szervezetére, ezen belül:

- szervezeti felépítésre,
- a bankbiztonsági szervezetre,
- a biztonsági szervezet tevékenységére, működésére, és annak szabályozottságára,
- a bankbiztonságra vonatkozó jogszabályoknak, külső szabályozóknak (PSZÁF, BASEL II., SOX) való megfelelőségére,
- az élőerős védelemre,
- a személyi védelemre,
- a mechanikai-fizikai védelemre,
- az elektronikai védelemre,
- a tűzvédelemre,
- a pénz- és értéktárolásra, szállításra,
- a pénzmosás elleni védelem belső szabályozottságának végrehajtására,
- a rendkívüli események (katasztrófák, terrorcselekmények) elleni védelemre,
- a humánerőforrás gazdálkodás biztonsági kérdéseire,
- a külső szerződéses partnerek bankon belüli mozgásával kapcsolatos kérdésekre,
- az ügyfél- és vendégforgalommal kapcsolatos kérdésekre.

A fenyegetettségek konkrét ismeretének hiányában az egyik lehetséges módszer a fenyegetések kockázatának megbecsülése, amely a fenyegetés által okozható legnagyobb kárérték és a fenyegetettségek az adott kárértékkel történő bekövetkezésének becsült gyakorisága (valószínűsége) szorzatával azonos. Ha a lehetséges kárértékeket és a bekövetkezési gyakoriságokat tartományokra osztjuk, akkor a kapott kockázati mátrixban meghatározhatók azok a kárérték-gyakoriság értékpárok, amelyek alatt a kockázat "elviselhető", illetve amely felett "nem elviselhető", azaz minden esetben konkrétan mérlegelendő a kockázat értéke és a csökkentését célzó védelmi intézkedések költségeinek egymáshoz való viszonya. Ez alapján lehet tervezés közben az azonos védelmi célú, de különböző védelmi szintű és költségű megoldásokat mérlegelni és kiválasztani. A tervezési feladat alapvető célja az, hogy minimális védelmi költségekkel a maximális kockázatcsökkentést tudjunk elérni.

KOCKÁZATELEMZÉSI MÓDSZERTAN

A vizsgálati módszer egy olyan modell, amelynek a középpontjában a védendő alapértékek (fizetőeszközök, értékpapírok, vagyontárgyak, információk, adatok, személyzet) állnak, amelyeket az értékek környezetét alkotó rendszerelemek vesznek körül. A fenyegetések, támadások a rendszerelemekre közvetlenül hatnak és az ezeken megvalósított védelem által realizált védelmi képességektől függően veszélyeztetett a védendő érték. A kockázat mértékét az egy időtávon belül felmerült fenyegetések gyakorisága és a védendő érték által hordozott kárérték szorzata határozza meg. Adott kockázati szinten a védelem erőssége szabja meg a fenyegetések "sikerességének" valószínűségét és az ezek során okozott kár összegét. Mivel a "sikeres" fenyegetések, támadások valószínűségét gyakorlatilag nem lehet nullára csökkenteni, minden szervezetnek meg kell határoznia azt a minimális kockázati értéket, azaz egy adott időtávra vetített kárösszeget, amelyet még el tud viselni, és ez határozza meg a szükséges védelmi szintet.

A kockázat meghatározása:

$$r = \sum_{t \in T} \left(p_t \times d_t \right),$$

ahol: **r**: a rendszer biztonsági kockázata [pl.: Ft/év],

T: a releváns fenyegetések halmaza,

$\mathbf{p_t}$: egy adott fenyegetés bekövetkezésének valószínűsége [pl.: 1/év],

$\mathbf{d_t}$: egy adott fenyegetés bekövetkezéséből származó kár [pl.: Ft]. [6]

A fenti modellre azért esett a választás más, sztochasztikus vagy determinisztikus kockázati modellekhez viszonyított pontatlansága ellenére a kvalitatív kockázatelemzéseknél[1] a gyakorlatban nagyon jól felhasználható. A vizsgálati módszer lépései azt célozzák meg, hogy végül hozzá lehessen rendelni minden rendszerelemhez a releváns fenyegetéseket, azok gyakoriságát és a védendő értékre jellemző és a vele funkcionális kapcsolatban levő rendszerelemekre vetített kárértéket. Az elviselhető kockázati határ ismeretében minden releváns fenyegetésre és minden felmért rendszerelemre már minősíthetők a kockázatok.

Ezek alapján a teljes vizsgálat elvégzése során a következő lépések [5] szerint érdemes haladni:

1. lépés: Tényhelyzet felmérés:
   - a védendő értékek meghatározása,
   - a védelmi igények és célok megfogalmazása,
   - a kárérték-osztályok meghatározása, kárértékek hozzárendelése a védendő értékekhez.
2. lépés: Fenyegetettség elemzés:
   - a veszélyeztetett rendszerelemek feltérképezése,
   - az alapfenyegetettségek és a rendszerelemek.
3. lépés: A fenyegető tényezők meghatározása:
   - gyenge pontok meghatározása a rendszerelemek területén,
   - a fenyegető tényezők meghatározása rendszerelem csoportonként,
   - rendszerelem-alapfenyegetés-fenyegető tényező összerendelés.

[1] Összetett rendszerek biztonsági kockázatainak vizsgálatához általában a kvalitatív kockázatelemzés kielégítő eredményt ad. Amennyiben kvantitatív kockázatelemzést kell végezni, a kockázat fenti definíciója – pontatlansága miatt – nem alkalmazható!

4. lépés: Kockázatelemzés:
   - kárértékek átvitele a rendszerelemekre,
   - a bekövetkezési gyakoriságok meghatározása,
   - a fenyegető tényezők és a bekövetkezési gyakoriságok összerendelése,
   - kockázati mátrix meghatározás,
   - kockázat minősítés a kockázati mátrix alapján.
5. lépés: Kockázat-kezelés:
   - a "nem elviselhető" minősítésű kockázati sorok összegyűjtése,
   - intézkedési javaslatok,
   - költségbecslés,
   - megvalósítás ütemezés, prioritások.

A fenti lépések szerint haladva egyrészt pontos képet kaphatunk egy pénzintézet biztonsági szempontok szerinti helyzetét illetően, valamint hatékony, széleskörű kockázatelemzést végezhetünk.

TÉNYHELYZETFELMÉRÉS

A vizsgálat során a bankbiztonság teljes körű vizsgálatát végezzük el, ehhez kapcsolódóan át kell tekintenünk a banknál megvalósuló alapfolyamatokat, a működés módját és a szabályozottságot, a szervezeti egységeket és azok tevékenységeit, bizonyos értelemben azokra szűkítve, amelyek a bankbiztonság szempontjából legfontosabb folyamatokat realizálják. Így behatárolhatóvá válnak azok az értékek, amelyek a bank folyamataiban meghatározók és így a bankbiztonság szempontjából érzékenyek.

A védendő alapértékek ez alapján meghatározhatóak és alapvetően három csoportba sorolhatók:

- fizetőeszközök, értékpapírok és vagyontárgyak,
- információk,
- személyek.

A védelmi célok feltérképezése, védelmi igények meghatározásához először is célszerű definiálni magának a biztonságnak a fogalmát. A biztonság értelmét, tartalmát sokan sokféleképpen magyarázzák. Elfogadva, hogy a biztonság egy *kedvező állapot*, amellyel szemben elvárható, hogy a fenyegetések bekövetkezésének lehetősége, valamint az esetlegesen bekövetkező fenyegetés által okozott kár a lehető legkisebb legyen. Ahhoz azonban, hogy teljes legyen ez a biztonság az szükséges, hogy minden valós fenyegetésre valamilyen védelmet nyújtson, ugyanakkor körkörös legyen, vagyis minden támadható ponton biztosítson valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy folyamatosan létezzen. [7]

A fentiek alapján *a biztonság a rendszer olyan – az érintett*[2] *számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.* Ahol a *zárt védelem* az összes releváns fenyegetést figyelembe vevő védelmet, a *teljes körű védelem,* pedig a rendszer valamennyi elemére kiterjedő védelmi intézkedések összességét jelenti. A *folytonos védelem* az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg. A *kockázattal arányos védelem* esetén egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel, azaz a védelemre akkora összeget és oly módon fordítanak, hogy ezzel a kockázat az érintett számára még elviselhető, vagy annál kisebb. [7]

[2] Az *érintett* alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő.

„A védelem akkor kielégítő erősségű (mértékű), ha a védelemre akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a releváns fenyegetésekből eredő kockázat (kárérték × bekövetkezési gyakoriság) a szervezet számára még elviselhető szintű vagy annál kisebb.” [8]

Hangsúlyozzuk, hogy a védelemre fordított költségeknek nemcsak az összege, hanem a ráfordítás módja is lényeges, azaz a védelmet teljes körűen és zártan kell kialakítani. A ráfordítás mértékét az elviselhető kockázat mértéke szabja meg, amelyet a kárérték és a bekövetkezési gyakoriság alapján meghatározott elviselhetőségi határ determinál. Ezt a határt minden szervezetnek egyedileg kell meghatároznia.

Egy szervezet biztonsági auditjának végső célja azon értékek biztonságának értékelése, amelyek egyéb veszélyeztetés tárgyai, illetve birtoklása a potenciális támadók célja és védelmük a tulajdonos alapvető érdeke. Minden esetben – így egy bank esetében is – vizsgálni kell, hogy milyen objektumok, milyen szempontból és milyen szinten képviselnek értéket a tulajdonos számára. A védelmi igények könnyebb meghatározása céljából ezt először általános szinten fogalmaztuk meg.

A hagyományos bankbiztonság szempontjából a védelmi célokat alapvetően két területen, az értékek tulajdonlása és a működőképesség területein fogalmaztuk meg, ezek sérülését vagy elvesztését tekinthetjük alapfenyegetettségeknek. Az értékek tulajdonlása területén az értékek a bank számára való tulajdonlásának, kezelésének, felhasználhatóságának biztosítását, a működőképesség területén az értékek rendelkezésre állásának és funkcionalitásának a biztosítását határozzuk meg alapvető védelmi célként.

A védelmi igények, azaz a szükséges védelmi szintek általános megfogalmazásához a megismert funkcionális folyamatok és működési mód alapján vizsgáltuk a védendő értékek és rendszerelemek természetét, tulajdonságait az alapfenyegetettségek szempontjából.

Ha az előzőekben megjelölt általános védelmi célok nem valósulnak meg, az adott bankot károk érhetik. Az audit során a károk tipizálását a következő területekre csoportosíthatjuk:

- közvetlen anyagi kár,
- közvetett anyagi kár,
- társadalmi, gazdasági-politikai jellegű károk,
- titok és adatvédelmi jogszabályok, előírások megsértése,
- személyi sérüléssel járó károk.

FENYEGETETTSÉG-ELEMZÉS

A védelmi igények feltárásakor egy pénzintézet objektumainak, illetve pénzintézeti tevékenységének és az ezekhez kapcsolódó értékek veszélyeztetettségét elemezzük és értékeljük.

A fenyegetettség elemzés során:

- feltérképezzük a veszélyeztetett rendszerelemeket,
- feltárjuk a védendő értékek és a rendszerelemek közötti függőségeket, amelyek segítségével megítélhetők a fenyegetések hatásmechanizmusai,
- meghatározzuk a rendszerelemek azon gyenge pontjait, amelyeken keresztül a fenyegetettségekből származó potenciális károkozás esélye magasabb szinten valószínűsíthető,
- feltérképezzük a rendszerelemekre ható fenyegető tényezőket.

Így megítélhető a rendszerelemekre és az értékekre ható fenyegetettségi kép, amely a rendszerelemekre – különösen azok gyenge pontjain át– a releváns fenyegetéseket foglalja magába.

A fenyegetett rendszerelemek feltárása során az értékek fenyegetettségének megítéléséhez a banki tevékenység és annak környezete minden olyan elemét figyelembe kell venni, amelyek valamilyen módon az értékekkel kapcsolatban vannak. Ezeket a továbbiakban rendszerelmeknek nevezzük. Ezeken keresztül az értékekre ható fenyegetések feltérképezéséhez kiinduló pont valamennyi olyan rendszerelem feltérképezése, amely valamilyen potenciális veszélynek van kitéve. A pénzintézeti biztonság szempontjából a veszélyeztetett rendszerelemek a következők:

- épület,
- közvetlen/támogató infrastruktúra (villamos és energetikai rendszerek, informatikai és távközlési hálózatok, raktárak, víz, csatorna, stb.),[9]
- banki tulajdonú berendezések, eszközök,
- készpénz és értékpapír tároló, feldolgozó helyiségek,
- vagyonvédelmi rendszerek,
- dokumentumok és dokumentáció,
- személyzet.

A bank biztonságát – az üzleti biztonságon kívül – többféle megközelítésben lehet értelmezni. A bankbiztonságot meghatározza a bank – ide értve minden az értékkezelésben résztvevő egységét – közvetlen környezete, a helyiségcsoportok kialakítása, azok megközelíthetősége, funkcionalitása, a telepített behatolás jelző-, tűzjelző-rendszer, valamint a videó-megfigyelőrendszerek, a dolgozók kiválasztása, a belső szabályozások és azok végrehajtása és nem utolsósorban a mobilizálható értékek (készpénz, értékpapír) tárolása, feldolgozása, szállítása, körülményei.

Érdemes külön megemlíteni, hogy a személyek elemcsoportot három egymástól jól elkülöníthető alcsoportra lehet bontani, ezek:

- a bank ügyfelei,
- a bankkal szerződéses jogviszonyban álló szervezetek, cégek dolgozói,
- a bank állományában dolgozók.

A korábban ismertetett védelmi modell szerint a fenyegetések végső célpontját azok a védendő alapértékek képzik, amelyeket a vizsgált szervezettől és az auditálás tárgyától függően mindig konkrétan meg kell határozni. Egy pénzintézet esetén esetében a következő alap kategóriákat vesszük figyelembe, mint védendő értékeket:

- fizetőeszközök, értékpapírok és vagyontárgyak,
- személyek,
- információk.

A felsorolt csoportokra ható konkrét fenyegetéseket általánosítva az alapfenyegetések két kategóriáját, a tulajdonlás, illetve a működőképesség elvesztését határoztuk meg és minden védendő alapértékhez a két alapfenyegetettség szerint rendelünk kárértéket. Ez a kárérték hozzárendelés meghatározó a kockázatelemzés során, mert a védendő alapértéket "körülvevő" rendszerelemekre - amelyekre a fenyegetések valamilyen gyakorisággal közvetlenül hatnak - ezek a kárértékek kerülnek rávetítésre.

A védendő alapértékek fenti kategóriái közül néhányat további csoportokra bontottunk, mert azok kárértékei egyrészt egymáshoz képest, másrészt az alapfenyegetettségek szempontjából lényegesen is eltérhetnek egymástól.

Az értékpapírok és az értéktárgyak banki, illetve nem banki tulajdonú alcsoportokra történő bontását a biztosítottság mértékében levő lényeges különbség indokolja.

A banki tulajdonú ingatlanok esetében a tulajdonost nagyobb kár sújtja, így a bankra nézve értelemszerűen a banki tulajdonú ingatlanokat ért károk dominánsak.

A berendezések és banki eszközök, mint tulajdon is komoly kárértéket képviselnek, de a bank működőképessége szempontjából is meghatározó szerepük van.

A személyek, mint védendő alapérték kategóriával kapcsolatosan ki kell térnünk egy különleges fenyegetésre, nevezetesen amikor emberi élet kerül közvetlen veszélybe, pl. bankrablás esetén. Ennek a fenyegetésnek a kockázat kezelése, az ezzel kapcsolatos intézkedések kívül esnek annak a védelmi modellnek a hatókörén, amelyet az korábban röviden ismertettünk. Az emberi élet közvetlen veszélyeztetésének elhárítása jóval magasabb prioritású minden más fenyegetés elleni védelemhez képest. Ebben az esetben elsődleges cél az emberi élet megmentése, azaz legmagasabb anyagi és/vagy erkölcsi kárt is el kell szenvednie a banknak, ha ezáltal az arra irányuló közvetlen fenyegetés elhárítható. Erre az esetre - mint ezt a banki szabályzatok is rögzítik - minőségileg más megfontolások és intézkedések lépnek életbe.

Az információknak két csoportját alakíthatjuk ki jogszabályi megfontolások alapján. A banktitkot tartalmazó információk, amelyek az ügyfelekre vonatkoznak és a bank üzleti titkait tartalmazó információk, amelyek a bank saját védendő értéke. A személyes adatok, ha azok az ügyfélre vonatkoznak banktitkot (is) jelentenek, ha saját alkalmazottra, akkor az üzleti titok csoportjába sorolhatjuk (logikailag, csak itt, de nem jogilag).

Egy bank védendő alapértékeinek a felsorolását az alábbi táblázat tartalmazza, amely azt tükrözi, hogy ezen alapértékekhez milyen kárértéket rendelünk a tulajdonlás és a működőképesség elvesztése esetén. A kárértékek nagyságát egy többfokozatú értékskála-rendszerbe soroljuk be. Érdemes páros számot választani, hogy az értékelés során a szakértőket egyértelmű állásfoglalásra késztessük. A kárértékek megállapításakor a biztosítások kárcsökkentő hatását célszerű figyelembe venni.

Sor-szám	Az alapérték megjelölése	a tulajdonlás	a működő-képesség
		értéke	
	készpénz és készpénz-helyettesítő fizetőeszközök		
	a bank tulajdonát képző értékpapírok		
	nem a bank tulajdonát képző értékpapírok		
	a bank tulajdonát képző ingatlanok (fiókok)		
	berendezések, banki eszközök		
	banktitkot képző adatok, információk		
	a bank üzleti titkát képző adatok, információk		

1. táblázat. Kárérték megállapításához alkalmazandó táblázat (készült az [5] alapján)

A FENYEGETŐ TÉNYEZŐK MEGHATÁROZÁSA

A védendő alapértékek alapfenyegetettségeihez kapcsolódó kockázatok megítéléséhez meg kell határozni az egyes rendszerelemekre, illetve elemcsoportra ható fenyegető tényezőket. A fenyegető tényezők legnagyobb valószínűséggel a rendszer gyenge pontjain keresztül tudnak érvényesülni. Az adott rendszerelemhez kapcsolódó kár kockázati tényezője így lesz reálisan megítélhető.

Egy bank biztonsági szempontból értelmezett gyenge pontjai a rendszerelemeket veszélyeztető károk fellépési valószínűségét növelik, illetve a védelmi intézkedések csökkentik.

Globálisan a fenyegetések három szintjét különböztetjük meg:

- gondatlan károkozás,
- szándékos, előre megfontolt, de egyedi károkozás,
- szervezett bűnözés (amely a szándékosan elkövetett bűncselekmények közül a legveszélyesebbnek tekintett).

Jelenleg elmondható, hogy mindhárom fenyegetés típus reális veszélyt jelent, mert – amint tapasztalható – a szervezett bűnözés is megjelent a hazai bankrendszerben. Ez a fenyegetési szint egy későbbi időszakban, a gazdasági és a pénzügyi élet egy magasabb fokán, illetve a szervezett bűnözés "magasabb intelligencia" szintjén fokozódni fog. Ezt a körülményt azért nem szabad lebecsülni, mert a szervezett bűnözés, mint professzionális támadó ellen minőségileg jóval magasabb szintű védelmet kell biztosítani, mint az első két típusú fenyegetés esetében.

KOCKÁZATELEMZÉS

A biztonsági vizsgálat eddigi lépései során a helyi sajátosságok figyelembevételével felmérésre kerülnek a védendő értékek a tulajdonlás, illetve a működőképesség elvesztése szempontjából. Megbecsüljük mind a két alapfenyegetettség szempontjából a hozzájuk kapcsolható kárértékeket. A fenyegetések közvetlenül a védendő értékeket "körülvevő" rendszerelemekre hatnak, ezért az alapértékekre becsült kárértékeket – mindkét alapfenyegetést sorba véve – rávetítjük a rendszerelemekre. Ezen értékek közül a legrelevánsabb alapfenyegetéshez tartozó kárértéket vesszük majd figyelembe az adott rendszerelemre ható fenyegetés által okozott kockázat meghatározásához.

Mint az előzőekben említettük a konkrét fenyegetések a rendszerelemekre hatnak, így a védelmi intézkedésekkel is elsősorban ezeket kell megcéloznunk. Rendszerelemnek nevezünk a rendszer vagy annak környezetét képző minden olyan elemet, amely valamilyen kapcsolatban (fizikai, logikai, funkcionális, szervezeti, stb.) van a védendő alapértékekkel. A védelem teljes körűségét és zártságát az biztosítja, hogy minden ilyen lehetséges rendszerelemet és az ezekre ható fenyegetéseket figyelembe vesszük és értékeljük. A mechanikai védelem eszközeit, az azokat magába foglaló rendszerelemmel együtt értékeljük.

A kárértékek meghatározásánál a meglévő biztosításokat nem vesszük figyelembe, mert bár jelentős kárcsökkentő hatása van a szervezetre nézve, a tulajdonos szempontjából ez nem egyértelmű a biztosítótársaságban való érdekeltsége miatt.

Egy adott fenyegetésnek egy rendszerelemre adódó kockázatát a rendszerelemre átvitt releváns kárérték és a káresemény becsült gyakorisága szorzata adja.

A rendszerelemekhez rendelve egyedileg határozhatóak meg azok a fenyegető tényezők, amelyek a vizsgált környezetben egyáltalán felléphetnek. Mivel valamennyi lehetséges fenyegető tényező ellen nem lehet tökéletes védelmet kialakítani, ezért ki kell választani a legfontosabb, azaz a bank működése szempontjából a legnagyobb kockázatot jelentő fenyegető tényezőket. Ehhez valamennyi feltárt fenyegető tényezőt értékelni kell. Az értékelés függ a fenyegetés valóra válása esetén, a lehetséges kár nagyságától és a kár bekövetkezésének várható valószínűségétől (gyakoriságától) – a kettő együttes értéke a kockázat.

A kárnagyság értékelésekor mérlegeljük, hogy az adott fenyegető tényező hatására milyen anyagi vagy más természetű károk következnek be, amelyek az ún. közvetlen károk és milyen későbbi következményekkel, úgynevezett következményes károkkal kell számolni.

A bekövetkezés várható gyakoriságára statisztikák, különösen a bűnügyi statisztikát, továbbá a műszaki hibák, a személyek akaratlan hibás tevékenysége miatt vagy vis maior esetek által bekövetkező károk gyakoriságának meghatározását a vonatkozó statisztikák alapján kell elvégezni. Nagyon fontos azonban a statisztikák használatakor annak vizsgálata, hogy azt ki, mikor és milyen célból készítette, mert a statisztikákat nem szabad kritika nélkül alkalmazni. Jelentős gondot okoz, hogy a statisztikai adatok mindig tartalmaznak bizonytalanságokat is.

A következő lépésben elvégzendő kockázat minősítéshez szükséges a releváns kárértékek és a gyakoriságok osztályai alapján adódó kockázati mátrixban annak a határvonalnak a meghatározása, amely felett a kárérték-gyakoriság értékpárokhoz tartozó kockázatot NEM ELVISELHETŐ-nek, az alatta levőket pedig ELVISELHETŐ-nek minősítjük. E határ-vonal megállapítását az adott szervezetre jellemző adatkategóriáknak, a hozzájuk tartozó kár-értékeknek és káresemény gyakoriságoknak az interjúk és az átadott dokumentumok elemzése határozza meg. E minősítés lesz az alapja a későbbiekben kiválasztandó védelmi intézkedésekre vonatkozó javaslatoknak.

A NEM ELVISELHETŐ kockázatok határát azon a becsült szinten, ahol a lehetséges kárnagyság, vagy a közvetett erkölcsi, politikai károk a bankok funkcionális működését egészében és alapvetően veszélyeztetik.

Minden korábban ismertetett fenyegető tényezőhöz a már felsorolt gyenge pontok súlyozott figyelembevételével külön-külön meghatároztuk, hogy a legnagyobb kár bekövetkezésével melyik alapfenyegetettség, mely rendszerelemen keresztül fenyeget és ez mekkora kárértéket (releváns kárérték) képvisel. Ezután táblázatos formában célszerű minden fenyegetéshez párosítottuk a rendszerelemet, amelyre az hat, a legjellemzőbb alapfenyegetést, a kockázat szintjét meghatározó releváns kárérték/káresemény gyakoriság számpárt valamint ezek figyelembevételével a kockázati mátrix (2. táblázat) alapján meghatározott kockázati minősítést (3. táblázat).

K	4^+	**E**	**N**	**N**	**N**	**N**	**N**
Á	4	**E**	**N**	**N**	**N**	**N**	**N**
R	3	**E**	**E**	**N**	**N**	**N**	**N**
É	2	**E**	**E**	**E**	**N**	**N**	**N**
R	1	**E**	**E**	**E**	**E**	**E**	**N**
T	0	**E**	**E**	**E**	**E**	**E**	**E**
É	-	**E**	**E**	**E**	**E**	**E**	**E**
K		0^-	0	1	2	3	4
GYAKORISÁGI ÉRTÉK							

2. táblázat. Kockázati mátrix (készült az [5] alapján)

A fenyegető tényező megnevezése	Az alap-fenyegetettség (… elvesztése)	A fenyegetett rendszerelem	Kárérték	Gy. érték	KOCKÁZAT

3. táblázat. Fenyegető tényezők kockázatának meghatározása táblázat (készült az [5] alapján)

KOCKÁZAT-KEZELÉS

A kockázat-kezelés során hozott intézkedések a kárnagyságot vagy a kárgyakoriságot csökkenthetik, és olyan hatásúaknak kell lenniük, hogy a NEM ELVISELHETŐ minősítésű kockázatok ELVISELHETŐ-vé mérséklődjenek. Az intézkedések alapvetően a rendszerelemek biztonsági jellemzőinek javítására irányulnak, de hatásuk a környezeti kapcsolódások miatt szélesebb területre terjed ki, olyan mértékben, hogy a védelem teljes körű és zárt legyen. Az intézkedések kiválasztásánál figyelembe vesszük azok kölcsönös, szinergikus hatásait. Az intézkedések megfogalmazását követően fontos a felelős személyek és tartható határidők megjelölése valamint a vizsgált területeket érintő változás esetén, illetve rendszeres időközönként történő felülvizsgálat elvégzése.

A CSOPORTMUNKA JELENTŐSÉGE A VIZSGÁLAT SORÁN

A biztonsági vizsgálat során célszerű csoportmunkában dolgozni, a hatékonyság érdekében. A csoport tagjainak kiválasztása során célszerű figyelembe venni a vizsgált terület összetettségét és minden érintett téma megfelelő szakértelemmel rendelkező képviselőjét bevonni a munkába. A megfelelő hatékonyság érdekében a csoportmunkában résztvevők száma célszerű, hogy 6-10 fő között legyen.

Mivel a munka során a csoport végzi az értékelést, elkerülhetetlen, hogy az „emberi” tényező nagy szerepet játszik az eredményben. A csoport segítségével azonban a szélsőséges vélemények megjelenésekor is ki lehet alakítani egy ésszerű kompromisszumot.

A csoporttagok a munka során a problémafeltárás és megoldás mellett számszerűsíthető értékeléseket is végeznek. Ebben az esetben számolnunk kell a csoportban működő különböző pszichológiai hatásokkal is (pl.: konformitás).[10] Mégis a munka során meghatározott értékek az amellett, hogy a csoport véleményét képviselik, segítenek a szubjektív álláspontokat közelíteni egymáshoz egy „átlag” meghatározásával. Így a szubjektív véleményekből egy kvázi objektív eredményre juthatunk. Persze a csoportösszetétel meghatározó a vizsgálat eredményét, eredményességét illetően.

ÖSSZEFOGLALÁS

A cikkben ismertettünk egy a pénzintézetek esetében jól alkalmazható kockázatelemzési módszertant, amelynek alkalmazása során vizsgálatra kerül a biztonsági rendszer zártsága, teljes körűsége és kockázattal arányos kiépítettsége, valamint a külső és a belső szabályozásoknak való megfelelés egyaránt.

A vizsgálat egy informatikai biztonsági kockázatelemzési módszertanon alapul, de ez a módszertan, mint a fentiekben is látható – megfelelő átalakításokkal – alkalmazható a pénzintézetek biztonságának vizsgálatára is. Bemutattuk, hogy e módszertan lépéseinek alkalmazása során csak a vizsgálat tárgyát kell megfelelően megváltoztatni ahhoz, hogy más (biztonsági) kockázatok elemzésére is alkalmas legyen.

A módszertannal szinkronban a pénzintézet biztonsági rendszere jelenlegi helyzetének felmérése után nemcsak a releváns fenyegetéseket és a védelmi rendszer gyenge pontjait kell vizsgálni, hanem a bank minden védendő alapértékére és az azt körülvevő rendszerelemekre vonatkozó kockázatokat is elemezni és minősíteni kell. Ez képezheti a szükséges biztonsági intézkedések kidolgozásának alapját.

Felhasznált irodalom

[1] The CCTA Risk Analysis and Management Method (CRAMM) User Guide, UK Government Central Computer and Telecommunications Agency (CCTA), IT Security and Privacy Group, 1993.

[2] BS IEC61882:2002 Hazard and operability studies (HAZOP studies) - Application Guide, British Standards Institution, 2002.

[3] MIL–HDBK–338B - Electronic Reliability Design Handbook : Fault Tree Analysis, Department of Defense (USA), 1998.

[4] MIL-STD-1629A - Procedures for performing a failure mode effect and criticality analysis, Department of Defense (USA), 1980.

[5] Balázs István, Déri Zoltán, Lobogós Katalin, Muha Lajos, Nyíri Géza, Sneé Péter, Váncsa Julianna: Informatikai Biztonság Irányításának Vizsgálata (IBIV), Miniszterelnöki Hivatal, 2008.

[6] Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna: A KIB 25. számú ajánlása: 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió, Miniszterelnöki Hivatal, 2008.

[7] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana: Az információbiztonság egy lehetséges taxonómiája, Bolyai Szemle XVII:4 (2008), 137-156.

[8] Bodlaki Ákos, Csernay Andor, Mátyás Péter, Muha Lajos, Papp György, Vadász Dezső: Informatikai rendszerek biztonsági követelményei, Miniszterelnöki Hivatal, 1996.

[9] Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren, HM Kommunikációs Szolgáltató Kht. – Zrínyi Kiadó, 2005.

[10] Tóth László: Pszichológia a tanításban, Pedellus Tankönyvkiadó, 2004.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Munk Sándor
munk.sandor@uni-nke.hu

AZ INFORMATIKAI IRÁNYÍTÁS ALAPJAI

Absztrakt

A korszerű informatika szolgáltatásai egyre inkább a társadalom, a gazdaság, a különböző tevékenységi területek és mindennapi életünk alapját, működési feltételét képezik. Az informatikai szolgáltatások alapját képező tevékenységek tervezettsége, szervezettsége, egységes irányítása alapvetően határozza meg a szervezetek, szakterületek, társadalmi tevékenységi szférák működésének eredményességét, minőségét. A szakirodalom eddig kevéssé foglalkozott az informatikai irányítás kérdéseivel olyan összetett szervezetrendszerekben, mint a közigazgatás és a védelmi szféra szervezetei. Jelen publikáció összegzi a vezetés, irányítás, felügyelet és ellenőrzés alapfogalmait; meghatározza a szakmai és ezen belül az informatikai irányítás fogalmát, értelmezését.

Modern IT services are increasingly necessary prerequisites, fundaments of the society, economics, different areas of activities, and our everyday life. Planning, organization, and direction of activities producing IT services fundamentally determines the operational effectiveness and quality of organizations, professional areas, social activity spheres. The professional literature so far hardly addressed the issues of IT management/control in such complex organizational structures, than public administration, and defense sphere organizations. Recent publication summarizes the basic concepts of management, control, and supervision; defines the concept and interpretation of professional, and IT management/control.

***Kulcsszavak**: vezetési funkciók, szakmai (szak-) irányítás, informatikai vezetés és irányítás ~ management functions, professional management/control, IT management and control*

BEVEZETÉS

Az informatika, a korszerű információtechnológia szolgáltatásai egyre inkább a társadalom, a gazdaság, a különböző tevékenységi területek és mindennapi életünk alapját, működési feltételét képezik. A technikai eszközökkel támogatott információs tevékenységek – információcsere, információszerzés, információ-előállítás, információellátás, stb. – nélkül a kialakulóban, kibővülőben lévő információs társadalom, a globális információs korszak működésképtelen lenne. Ez a sokak által korszakváltásnak tekintett folyamat, amely erőteljesebben valahol a múlt század utolsó harmadában indult meg, napjainkban egyre gyorsuló ütemben halad előre.

Az átmenet alapját az információs szolgáltatások körének, mennyiségi és minőségi jellemzőinek, elérhetőségének – az információtechnológia fejlődésére épülő – bővülése képezi. A szolgáltatások mögött a hagyományos ágazatokat (ipar és mezőgazdaság) megközelítő jelentőségű információs szektor, információs folyamatok és tevékenységek, "információs munkások" állnak. Az információs tevékenységek az önálló információs folyamatok mellett át és átszövik a hagyományos működési folyamatokat is, tervezettségük, szervezettségük, egységes irányításuk alapvetően határozza meg szervezetek, szakterületek, társadalmi tevékenységi szférák működésének eredményességét, minőségét.

A szervezeti célkitűzéseket támogató informatikai – vagyis a technikai támogatással megvalósuló információs – szolgáltatások megvalósulásának és hasznosulásának feltétele az informatikai tevékenységek vezetése és irányítása. E két fogalom széles körben elfogadott értelmezésére támaszkodva jelen publikációban informatikai vezetés alatt informatikai rendeltetésű szervezet vezetését, informatikai irányítás alatt pedig informatikai tevékenységekre a szervezeten, szervezeti elemen kívülről – a későbbiekben részletezendő módon – hatást gyakorló vezetési tevékenységet értünk.

Olyan összetett szervezetrendszerekben, mint a közigazgatás rendszere, a védelmi szféra intézményei (Magyar Honvédség, Magyar Rendőrség, a katasztrófavédelem rendszere) az informatikai irányítás, mint a vezetés és működés feltételeit biztosító tényező lényeges szerepet játszik, így alapvető kérdéseinek vizsgálata érdeklődésre tarthat számot. Ennek ellenére az informatikai irányítás – fenti, átfogó értelemben vett – fogalmával, tartalmával foglalkozó tudományos és szakmai publikációk köre rendkívül szűkös.

A szakirodalomban az informatikai irányítás (IT governance) az információs és kapcsolódó technológiák ellenőrzési eljárásainak célkitűzései (COBIT[1]) keretrendszer alapvető fogalmaként jelent meg. Eszerint "az informatikai irányítás a felső vezetés és az igazgatótanács felelőssége, és az informatikai irányítás lefedi azokat a területeket – a vezetést, a szervezeti struktúrát és folyamatokat – amelyek biztosítják, hogy a vállalat informatikai szolgáltatásai hozzájáruljanak a szervezet stratégiáinak és célkitűzéseinek fenntartásához és kiterjesztéséhez." [1, 9. o.] Mint a definícióból is látható, a COBIT fogalom a tartalmat alapvetően a felső vezetés teendőire szűkíti.

Hasonló értelmezést takar a felsőszintű informatikai irányítás (corporate governance of IT) fogalma is, amely a 2000-es évek elején bekövetkezett tőzsdei válságokra, köztük a 'dotcom buborék kipukkadására'[2] adott válaszként megjelent [felelős] szervezeti irányítás (corporate governance) kereteibe illeszkedően. Eszerint a felsőszintű informatikai irányítás az informatika jelenlegi és jövőbeni felhasználását irányító és felügyelő rendszer, amelynek összetevői: a szervezetet támogató informatika-alkalmazás értékelése és irányítása, valamint a

[1] Control Objectives for Information and Related Technology.
[2] A túlértékelt informatikai, elsősorban az Internet-szektorhoz kapcsolódó társaságok jelentős tőzsdei értékvesztése.

tervek megvalósításának figyelemmel kísérése. Magában foglalja továbbá a szervezeti informatika-alkalmazás stratégiáit és irányelveit. [2, 3. o.]

Az említett két megközelítés mellett olyan átfogó informatikai irányítási értelmezés, vizsgálat, amely alapjául szolgálhatna az informatikai szakmai irányítás feladatai átfogó tárgyalásához, a magyar szakirodalomban nem jelent meg. A fentiek alapján jelen publikáció alapvető célja, hogy feltárja és meghatározza az általános értelemben vett informatikai irányítás alapjait. Ezen belül:

- összegezze az irányítás, vezetés, felügyelet és ellenőrzés alapfogalmait;
- elemezze a szakmai irányítás és felügyelet fogalmát, tartalmát;
- meghatározza az informatikai irányítás, mint szakmai irányítás, fogalmát, helyét és szerepét, kapcsolatrendszerét.

AZ IRÁNYÍTÁS ÉS A KAPCSOLÓDÓ VEZETÉSI FUNKCIÓK

Az irányítás a célirányos, tervszerű és szervezett (társadalmi, gazdasági, szervezeti, stb.) folyamatok nélkülözhetetlen eleme. Az irányítás fogalmának számos különböző értelmezésével találkozhatunk, amelyek ezek általában megegyeznek abban, hogy az irányítás olyan tevékenység, amely során az irányító meghatározó befolyást gyakorol az irányított (szervezet, rendszer, folyamat) működésére, tevékenységére, lefolyására. Egyetértés van abban is, hogy az irányítás mindig az irányított szervezeten, rendszeren kívülről történik, a működés, tevékenység befolyásolása kívülről történő ráhatással valósul meg. A következőkben megfogalmazottak alapvetően a közigazgatási irányítás, felügyelet és ellenőrzés széles körben elfogadott megállapításaira alapulnak. [Részletesebben lásd például: 3]

Az irányítás fogalma, tartalma

Szervezetek – szervezeti folyamatok, tevékenységek – irányításához megfelelő jogosultságra van szükség, amely az irányító és az irányított szervezet meghatározott erősségű hierarchikus viszonyt (alá- és fölérendeltséget) feltételez. A közigazgatási jog szerint az *irányítás* olyan jogviszony, amelyben jogszabály által irányítási jogkörrel felruházott, az irányítottól elkülönült szervezet az irányított szervezetek részére – egyértelműen, jogszerű akaratnyilvánítási formában (döntés) – reális célokat, teljesíthető feladatokat (magatartást) határoz meg. A végrehajtást az irányító jogosult és köteles felügyelni, ellenőrizni, a cél elérése, a feladat végrehajtása érdekében szükség esetén kényszereszközöket alkalmazhat. Az irányítási joghoz kötelesség is társul, az irányítónak a cél elérése, a feladat megvalósítása érdekében a szükséges erőforrások elérhetőségéről, a megvalósítás információs és szervezeti feltételeiről gondoskodnia kell.

Az *irányítás tárgya* körébe az irányított szervezet szervi és szakmai ügyei tartoznak. A szervi ügyek a szervezet létével kapcsolatos viszonyokat foglalják magukban (alapítás, átszervezés, munkáltatói jogok, pénzügyek stb.), míg a szakmai ügyek csoportját azok a tevékenységek alkotják, amelyek ellátására a szervezetet létrehozták.

Az *irányítási jogviszony tartalma* az irányító számára rendelkezésre álló jogosítványok összessége. Ezek lehetnek jogi (irányítási) eszközök és egyéb cselekmények. Az irányítás jogi eszközei közé tartoznak:

- normatív (általános érvényű) szabályozások: jogszabályok, a közjogi szervezetszabályozó eszközök, belső rendelkezések;
- konkrét utasítások: egyedi jellegű feladat-meghatározó, kötelezettséget előíró előírások;
- egyedi (általában szervi) döntések: amikor az irányító átveszi az irányított szerv döntési jogát, vagy azzal megosztja azt (véleményezés, előzetes hozzájárulás, utólagos jóváhagyás, javaslatkérés);
- döntések/aktusok felülvizsgálata: jogsértő, vagy célszerűtlen döntések/aktusok megsemmisítése, megváltoztatása;
- végül az ellenőrzés.

Az egyéb cselekmények nem jogi eszközök, azonban lehetnek jogilag szabályozottak. Ide tartoznak pld. a következők: tájékoztatás, feladatok megmagyarázása, gyakorlati segítségnyújtás, erkölcsi és anyagi ösztönzés, továbbképzés.

Irányítás és vezetés

Az irányítás alapjainak bemutatása során meg kell határozni viszonyát a vezetéshez, amellyel szoros kapcsolatban áll és a gyakorlatban egymástól nem mindig pontosan határolódik el. Szervezetek esetében a vezetés olyan tevékenység, amely során a vezető a vezetett szervezet tagjaként (az irányító által meghatározott feladatok végrehajtása érdekében) meghatározó befolyást gyakorol a szervezet tevékenységére. Ennek során a szervezet tevékenységének célját és rendeltetését nem változtathatja meg.

Szervezetekben az eredményes vezetés megvalósításához természetesen megfelelő jogosultságokra van szükség. Ebből a szempontból egy adott szervezeten belül a vezetés olyan jogviszony, amely a vezetettekkel azonos jogviszonyban álló személyt, vagy testületet ruház fel vezetői jogkörrel és egyben felelősséggel. A vezetés joga kizárólag az arra kijelölt személyt, vagy testületet illeti meg. Ezt a jogot, az ennek részét képező jogköröket, meghatározott keretek között megoszthatja, átruházhatja, azonban vezetői felelőssége ettől függetlenül fennáll.

A vezetés alapvetően emberekre irányuló tevékenység, ráhatás, befolyásolás annak érdekében, hogy a vezetettek megértsék, elfogadják és maradéktalanul végrehajtsák a szervezet vezetőjének döntéseit, aki ezek segítségével közvetíti a szervezet személyi állománya részére az irányító által kitűzött célokat, előírt feladatokat. Ennek keretében meghatározza a részcélokat, részfeladatokat, a megvalósításhoz célszerű magatartást. Megszervezi a megvalósításhoz szükséges munkamegosztást, kialakítja és folyamatosan fenntartja a tevékenység feltételeit, ellenőrzi a folyamatokat, figyelemmel kíséri a végrehajtást és megteszi a szükséges beavatkozásokat a feladatok szakszerű, hatékony végrehajtásának biztosítására.

Hierarchikus szervezetekben, összetett szervezetrendszerekben az irányítás és a vezetés szintenként váltakozó módon kapcsolódik egymáshoz. A szervezet vezetője – vezetői jogkörében – irányítja helyettesei, más közvetlen alárendeltjei, esetleg egyes szervezeti egységek vezetőinek tevékenységét. Ez utóbbiak vezetik saját szervezeti egységüket (pld. főosztály, csoportfőnökség, stb.) és ezen belül irányítják az alacsonyabb szintű szervezeti elemek (pld. osztály) vezetőinek tevékenységét.

Az irányítás és a vezetés részelemei (informálódás, tervezés, döntés, szervezés, feladatszabás, feltételek megteremtése, ellenőrzés, beavatkozás) jelentős azonosságot, átfedést mutatnak. A különbségek elsősorban a következőkben jelentkeznek:

- az irányító az irányított szervezeten kívül helyezkedik el, a vezető része a szervezetnek;
- az irányító módosíthatja az irányított célját, feladatait, státuszát, struktúráját, a vezető a meghatározott célokon, feladatokon általában nem változtathat, a státusz, struktúra módosítását csak kezdeményezheti;
- az irányító a szervezet tagjai esetében csak általános feltételeket határozhat meg, egyedi ügyekben nem dönthet, felettük a munkáltatói jogokat a vezető gyakorolja.

Irányítás, felügyelet és ellenőrzés

Az irányítás szempontjából a vezetés mellett szükség van a felügyelethez, valamint az ellenőrzéshez kapcsolódó viszonyának meghatározására is. Általában elfogadott nézet, hogy a felügyelet az irányításnál szűkebb jogkört foglal magában, egyes nézetek szerint a felügyelet az irányítás egy részjogosítványa.

Az irányítás alapvető összetevője a döntés, a cél- és feladat-meghatározás. Ezek a gyakorlat szerint nem képezik részét a felügyeletnek, amelynek lényegét a figyelemmel kísérés, ellenőrzés és szükség esetén a beavatkozás (intézkedés) jelenti. A közigazgatási jog szerint a *felügyelet* olyan jogviszony, amelyben a felügyeleti jogkörrel felruházott, a felügyelttől elkülönült szerv, szervezet gondoskodik arról, hogy a felügyelt szervezet működése megfeleljen az előírt magatartásnak.

A felügyeletet gyakorló figyelemmel kíséri, ellenőrzi a felügyelt szervezet tevékenységét és szükség esetén gondoskodik az előírt magatartás kikényszerítéséről, vagy ilyen intézkedést kezdeményez az arra jogosult szervezetnél. Nem terjed ki tehát a felügyelet a cél, a feladat, vagy a magatartás meghatározására, illetve az ezeken kívül eső magatartási formák kikényszerítésére.

A felügyeletet gyakorló különböző eszközök segítségével szerezhet információkat a felügyeltek tevékenységéről. Ezek közé tartozik például: a rendszeres adatszolgáltatás, a meghatározott feltételhez kötött jelentési/tájékoztatási kötelezettség, az egyedi információkérés/beszámolási kötelezettség, valamint a felügyelt szervezeten kívüli információk (panaszok, bejelentések, stb.). A felügyeleti intézkedés lehet kötelező (tiltó), szankcionáló, vagy eljárást kezdeményező tartalmú.

Az *ellenőrzés* a felügyeletnél is szűkebb jogkör és tevékenység, amelynek során az ellenőrző a meghatározott előírások, célok, feladatok ismeretében megvizsgálja és értékeli az ellenőrzött tevékenységét, elért eredményeit. Az ellenőrzés nem foglal magában beavatkozási jogot, az ellenőrző szükség esetén csak más szerv eljárását, intézkedését kezdeményezheti. Az ellenőrzési jog összetevői közé tartoznak: a tájékoztatáskérés, az iratbekérés és a helyszíni ellenőrzés (belépési lehetőség, iratok, tárgyak, munkafolyamatok megtekintése, mintavétel, stb.).

SZAKMAI IRÁNYÍTÁS, INFORMATIKAI IRÁNYÍTÁS

A szakmai irányítás, felügyelet alapjai

Az irányítás fogalma összetett szervezetrendszerekben szorosan kapcsolódik a szervezetek alá-fölérendeltségi (hierarchikus) viszonyaihoz. Ezek esetében egy magasabb szintű szervezet az alárendeltségébe tartozó szervezetek felett jellemzően teljes irányítási hatáskörrel

rendelkezik. Ez a szervezetek önállóságának növelése érdekében korlátozható a hatáskör elvonásának tilalmával, a konkrét utasítási jog korlátozásával, vagy kizárásával, illetve az aktus-felülvizsgálati jog korlátozásával.

Irányítási viszonyok összetett szervezetrendszerekben nem csak a hierarchikus alá-fölérendeltségi kapcsolatok mentén lehetségesek, létezik az úgynevezett *hierarchián kívüli irányítás* fogalma is, amely lényegét tekintve nem alárendelt szervezet feletti irányítási jogosítványok összessége. A hierarchián kívüli irányítás a hierarchikus irányítással szemben jelentősen korlátozott, alapvető jellemzője, hogy csak az irányított szervezet szakmai ügyeire, tevékenységére terjed ki. Közigazgatási területen megnevezése ágazati irányítás, szervezetrendszeren/szervezeten belül pedig szakmai irányítás.

A *szakmai irányítás (szakirányítás)* meghatározott szakterülethez tartozó ügyekre, tevékenységekre vonatkozó irányítási jogkörök és azok gyakorlásának összessége, vagyis egy adott szakterületre kiterjedő irányítás. A szakmai irányítás rendeltetése az irányított szervezetek adott szakterülethez tartozó tevékenységeinek (szaktevékenységeinek) az alaprendeltetést, az általános célkitűzéseket támogató, eredményes és hatékony megvalósításának biztosítása.

A szakmai irányítás hatálya alá tartozik a szervezetrendszer minden olyan szervezete, amelyben folyik szaktevékenység. Ennek megfelelően a szakmai irányítás nem feltétlenül tisztán hierarchián kívüli irányítás, mivel az irányított szervezetek közül – bár többségük jellemzően alárendeltségen kívüli – lehetnek a szakmai irányító alárendeltségébe tartozó (szakmai) szervezetek is.

Összetett, hierarchikusan mélyen tagolt szervezetrendszerekben a szakmai irányításnak – az alá-fölérendeltségi viszonyokhoz kapcsolódó irányításhoz hasonlóan – lehetnek különböző szintjei. Ebben az esetben a felső szintű szakmai irányítás a szervezet és a szakterület egészére kiterjedő felelősséggel és jogkörrel rendelkezik. Az alacsonyabb szintű szakmai irányítás típusai közé tartozhat a szervezeti hierarchiához igazodó, a szervezet egy részére kiterjedő középszintű szakmai irányítás, valamint a szakmai részterületre korlátozódó funkcionális szakmai irányítás.

A *szakmai felügyelet (szakfelügyelet)* a szakmai irányítás (szakirányítás) részét képező tevékenység, az adott szakterületre (szaktevékenységekre) vonatkozó szabályozók érvényesülésének ellenőrzése és szükség esetén intézkedés ezek érvényre juttatására. A felügyelet további típusai közé tartozik a törvényességi felügyelet, amely kizárólag jogszabálysértések orvoslására hivatott és a hatósági felügyelet, amely az állampolgárokat, szervezeteket érintő hatósági eljárások felügyeletét jelenti.

Az informatikai (szakmai) irányítás fogalma, tartalma

Az előzőekben foglaltaknak megfelelően a szakmai irányítás (szakirányítás) fogalma értelmezhető az informatikai szakterület, az informatikai tevékenységek esetében is. Ennek megfelelően *informatikai (szakmai) irányítás* alatt – egy adott szervezeten belül, vagy egy állam esetében – az informatikai szakmai ügyekre, tevékenységekre vonatkozó irányítási jogkörök és feladatok összességét értjük. Az informatikai (szakmai) irányítás rendeltetése az irányított szervezetek informatikai tevékenységeinek az alaprendeltetést, a szervezeti célkitűzéseket támogató, eredményes és hatékony megvalósításának biztosítása.

Informatikai tevékenység alatt az informatikai eszközök, rendszerek szolgáltatásainak a szervezeti célkitűzéseket szolgáló, hatékony igénybevételére, valamint az informatikai szolgáltatások feltételeinek kialakítására (továbbfejlesztésére) és fenntartására irányuló tevékenységeket értünk. E tevékenységek között vannak speciális ismereteket és felkészültséget, informatikai szakemberek közreműködését nem igénylő általános

informatikai tevékenységek és speciális szakismereteket, informatikai szakemberek közreműködését igénylő informatikai szaktevékenységek.

A szakmai irányítás, így az informatikai (szakmai) irányítás – mint irányító és irányított közötti (jog)viszony – nem önmagáért és önmagában való, részét képezi a szervezeti vezetésnek, amelynek rendeltetése a szervezet eredményes és hatékony működése feltételeinek megteremtése. Az informatikai irányító szerv (vezető, szervezeti egység) a vezetési rendszeren belül a szervezet rendeltetésétől, a választott szervezeti/vezetési struktúrától, az informatikai szolgáltatások, tevékenységek szervezetben betöltött szerepétől, jelentőségétől stb. függően – más szakterületekhez hasonlóan – különböző tartalmú, terjedelmű feladat- és hatáskörökkel rendelkezhet.

ÖSSZEGZÉS

A vezetés, irányítás, felügyelet és ellenőrzés fogalma, tartalma viszonylag egységes értelmezésben szerepel a közigazgatás-tudományi, közigazgatási jogi szakirodalomban. Ennek megfelelően a *vezetés* egy szervezeten belüli fogalom, a szervezet vezetője és a szervezet tagjai közötti jogviszony (egyben feladatrendszer). Az *irányítás* pedig szervezetek közötti jogviszony (feladatrendszer), amely során az irányító meghatározó befolyást gyakorol az irányított (szervezet, rendszer, folyamat) működésére, tevékenységére, lefolyására. A *felügyelet* az irányításnál szűkebb jogkört foglal magában, annak részjogosítványának is tekinthető. A felügyelet lényegét tekintve a felügyeltek tevékenységének, a szabályozók és az irányítás által előírtak megvalósulásának figyelemmel kísérése és eltérés esetén beavatkozás. A beavatkozásnak, intézkedésnek a felügyeleti jogkör tartalmától függően különböző jellegű és erősségű megoldásai lehetségesek. Az *ellenőrzés*, mint külső jogviszony, a felügyeletnél is szűkebb jogkör és tevékenység, amely nem foglal magában beavatkozási jogot, az ellenőrző szükség esetén csak más szerv eljárását, intézkedését kezdeményezheti.

Összetett szervezetrendszerekben, mint amilyen a közigazgatási szervezetrendszer és amilyenek védelmi szféra szervezetei, az irányítás alapvetően egy hierarchikus alá-fölérendeltségi struktúrához kapcsolódik. Emellett azonban létezik a *hierarchián kívüli irányítás* fogalma is, amely lényegét tekintve nem alárendelt szervezetek feletti, a hierarchikus irányítással szemben jelentősen korlátozott jogosítványok összessége és csak az irányított szervezetek szakmai ügyeire, tevékenységére terjed ki.

A *szakmai irányítás (szakirányítás)* meghatározott szakterülethez tartozó ügyekre, tevékenységekre vonatkozó irányítási jogkörök és azok gyakorlásának összessége, egy adott szakterületre kiterjedő irányítás. Rendeltetése az irányított szervezetek adott szakterülethez tartozó tevékenységeinek (szaktevékenységeinek) az alaprendeltetést, az általános célkitűzéseket támogató, eredményes és hatékony megvalósításának biztosítása. A *szakmai felügyelet (szakfelügyelet)* a szakmai irányítás (szakirányítás) részét képező tevékenység, az adott szakterületre (szaktevékenységekre) vonatkozó szabályozók érvényesülésének ellenőrzése és szükség esetén intézkedés ezek érvényre juttatására.

Végül *informatikai (szakmai) irányítás* alatt informatikai szakmai ügyekre, tevékenységekre vonatkozó irányítási jogkörök és feladatok összességét értjük, amelynek rendeltetése az irányított szervezetek informatikai tevékenységeinek az alaprendeltetést, a szervezeti célkitűzéseket támogató, eredményes és hatékony megvalósításának biztosítása. Informatikai tevékenységek mindazon tevékenységek, amelyek az informatikai eszközök, rendszerek szolgáltatásainak a szervezeti célkitűzéseket szolgáló, hatékony igénybevételére, valamint az informatikai szolgáltatások feltételeinek kialakítására (továbbfejlesztésére) és fenntartására irányulnak.

Felhasznált irodalom

[1] COBIT 4.1 Magyar változat (1.3 változat – első nyilvános verzió) – ISACA Budapest Chapter, 2007.

[2] ISO/IEC 38500:2008(E), Corporate governance of information technology. – ISO/IEC, 2008.06.01.

[3] HORVÁTH Attila (szerk.): Irányítás, felügyelet és ellenőrzés a közigazgatás működésében. Tankönyv a köztisztviselők továbbképzéséhez. – Magyar Közigazgatási Intézet, Budapest, 2007. május.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Papp Zoltán
pappz.szeged@gmail.hu

AZ INFORMÁCIÓ TÁMADÁSA ANNAK TULAJDONSÁGAIN KERESZTÜL

Absztrakt

Fejlett korunkban a társadalmi, a gazdasági, illetve a rendvédelmi szektor működésében az információ központi szerepet tölt be, így annak megfelelő minősége elengedhetetlenül fontos ahhoz, hogy a döntés-előkészítő, a döntéshozó, illetve a végrehajtó folyamatok hatékonysága az igényeknek megfelelő legyen. Az adat, az információ a keletkezéstől a felhasználásig számos munkafolyamaton keresztül alakul át, ahol az eltérő indíttatású támadóknak – fázisonként különböző módszerrel, akár technikai, akár kognitív dimenzióban – lehetőségük van arra, hogy az adat, az információ különböző jellemzőit módosítsák, ezáltal gyakorolva hatást az adatgyűjtő, elemző, döntéshozó és végrehajtó folyamatokra.

Information has a central role in the functioning of the social, economic and law enforcement sectors in our modern age, therefore its appropriate quality is of utmost importance for operating efficient decision support, decision making and executive processes. From its creation until its actual usage, data and information undergo several work processes during which attackers of various motives – applying different methods in each phase either in the technical or the cognitive dimensions – are able to modify certain parameters of the data and information, thus impacting the data collecting, analyzing, decision making and executive processes.

Kulcsszavak: *információ, támadás ~ information, attack*

BEVEZETÉS

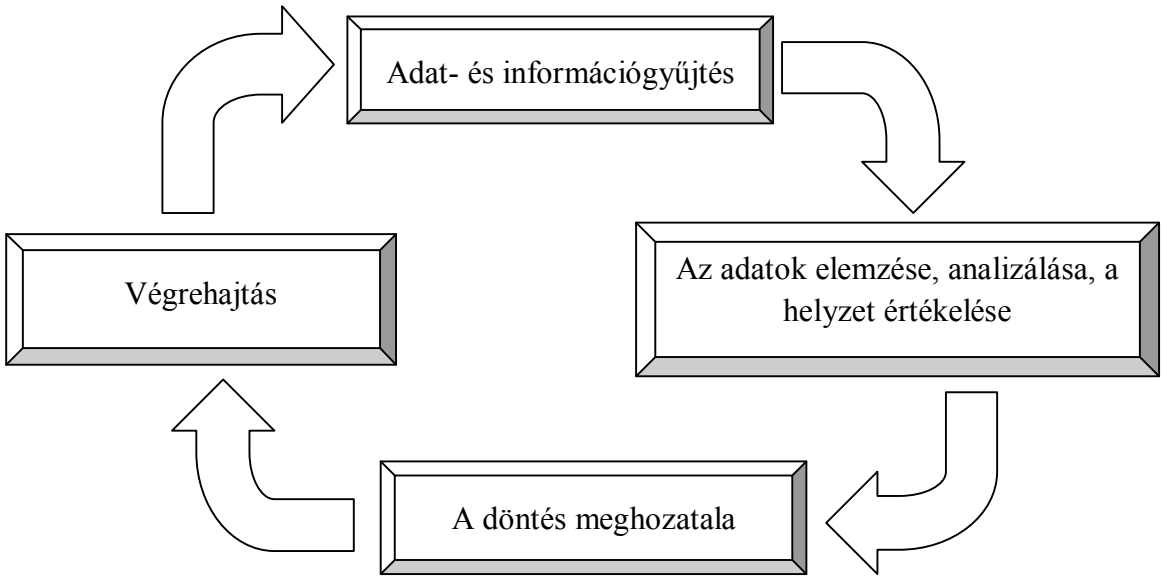
Az információ latin eredetű szó, amely értesülést, hírt, üzenetet, tájékoztatást jelent. Egyben az informatika alapfogalma. Számos jelentése, kifejtése köztudott, különböző tudományágak különböző módon közelítik meg, írják le. Egyértelműen elfogadott definíciója nem ismert. Általánosságban információnak azt az adatot, hírt tekintjük, amely számunkra releváns és ismerethiányt csökkent. Az egyik legleegyszerűsítettebb megfogalmazás szerint az információ nem más, mint valóság (vagy egy részének) visszatükröződése. [1] Tudományos értelmezését az információelmélet fogalmazza meg.

Az adat magában sem jelentéstartalommal, sem információval nem bír. A jelentéstartalom az adatra vonatkozó valamilyen értelmezési szabályokat feltételez, és az adat ilyen szabályok szerinti értelmezése vezet a jelentéstartalomhoz. A jelentéstartalom pedig csak akkor szolgál információval az értelmező számára, ha azzal ő új ismeret birtokába kerül. [2]

Az információs társadalomban ahhoz, hogy az egyének, illetve szervezeteik, szerveződéseik az életüket, tevékenységüket hatékonyan, gazdaságosan és célszerűen tudják irányítani információkra van szükségük, mégpedig pontosan azokra információkra, amelyek ezekhez a feltételekhez szükségesek. Az információnak – hogy szerepét, fontosságát betöltse – mindig a megfelelő helyen, a kellő időben, a kívánt tartalommal és célszerű formátumban kell rendelkezésre állnia. Mint látszik, a felhasználó szempontjából több feltétel egyidejű megléte esetén hasznosítható csak az információ. Ha az információ, illetve annak valamely tulajdonsága nem felel meg a felhasználó – akár egy személy, akár egy szervezet – igényeinek, akkor az hatással lesz a döntés kimenetelére, vagy akár a végrehajtás minőségére is.

A VEZETÉSI CIKLUS

A különböző entitások az adatokkal, az információkkal kapcsolatos tevékenységüket az információs környezet különböző dimenzióiban végzik. A számukra szükséges információkat különböző tulajdonságú, pontosságú és megbízhatóságú forrásokból szerzik be, amelyeket aztán saját szempontrendszerük alapján feldolgozzák, elemzik, értékelik. Az értékelési szakaszt követően az egyének, illetve a szervezetek céljaik elérése, küldetésük betöltése érdekében döntési alternatívákat állítanak fel, majd a rendelkezésre álló erőforrásaik, lehetőségeik függvényében meghozzák a számukra legoptimálisabbnak tűnő döntést. A döntési folyamat lezárultával kezdődnek el a célok elérése érdekében kezdeményezett műveletek, melyeket akár a fizikai, akár az információs térben egyaránt végrehajthatnak. A végrehajtás minőségét, hatékonyságát a pontos és hiteles információk nagyban képesek növelni. A végrehajtott műveletek értelemszerűen hatást gyakorolnak a környezet különböző dimenzióira, melyből lehet következtetni a műveletek eredményére. A hatás felmérése, illetve a további intézkedések megtétele érdekében a fentebb vázolt információgyűjtés - értékelés - döntés - végrehajtás – úgynevezett vezetési ciklus – újrakezdődik [3:167]:

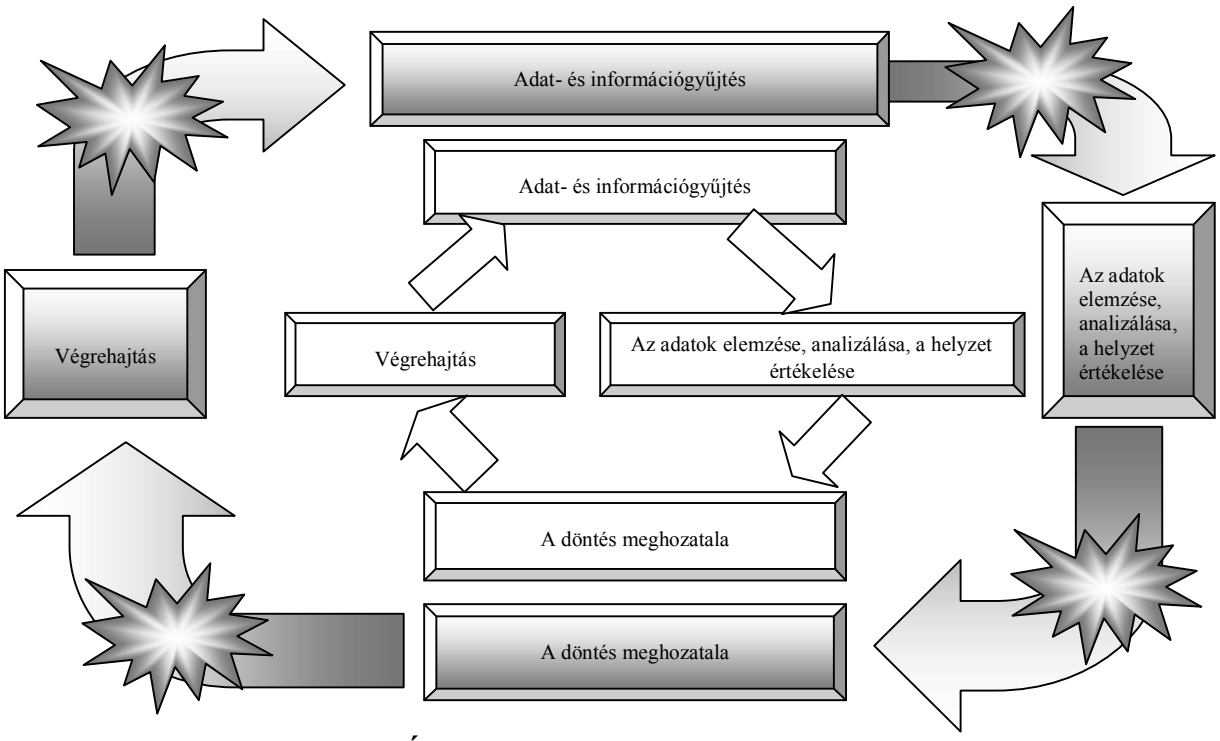


1. Ábra. A vezetési ciklus [3:167]

A ciklusban feltüntetett pontok által végzett munka eredményességére kihatással van az előző folyamatok tevékenységének, információinak minősége. A ciklusba bekerülő adatok, információk pontossága, hitelessége a feldolgozás során torzulhat

A ciklus meghatározott idő alatt zajlik le, mely nagyban összefügg az entitás információgyűjtő lehetőségeivel, a helyzetet elemző, értékelő szakemberek képzettségével, a vezetők tapasztalatával és a végrehajtók rutinjával, képességeivel, valamint a minden munkafázis mögött meghúzódó technikai, informatikai, kommunikációs eszközök fejlettségével. Amennyiben a környezet a vezetési ciklus időintervallumánál gyorsabban változik, akkor a döntéshozatal során meghozott döntések már nem a valós helyzetre reagálnak, és ez a körülmény a végrehajtás hatékonyságát is jelentősen ronthatja, sőt akár hatástalanná is teheti, így ahhoz, hogy egy szervezet saját helyzetét, pozícióját a saját környezetében pontosan ismerje a fenti ciklust a lehetőségeinek függvényében minél többször szükséges végrehajtania.

Ha ugyanabban a környezetben két ellenérdekelt fél tevékenykedik, melyek lehetnek akár szembenálló hadseregek, vagy akár gazdasági társaságok, illetve egyéb felek (például rendészeti szervek és terrorcsoportok), akkor elemi érdekük, hogy a pontos helyzetismeret érdekében vezetési ciklusuk idejét csökkentsék. Az időért folytatott harcban a feleknek több lehetőség is rendelkezésükre áll. Egyrészt saját szervezetük és technikai eszközeik hatékonyságának növelésével vívhatnak ki maguk számára előnyt, azonban az ebben rejlő lehetőségek korlátozottak, másrészt irányként megfogalmazódhat, hogy az ellenérdekelt fél információs folyamataiba beavatkozva növeljék annak ciklusidejét, rontsák az ottani rendszerben kezelt információk minőségi jellemzőit, mellyel a vezetés hatékonyságát csökkenthetik [3:167].



2. Ábra. A vezetési ciklus [3:167]

Az információs folyamatokba történő beavatkozás eredményét három tényező befolyásolja jelentősen:

- A támadó mekkora támadási potenciál birtokában van. Ez azt mutatja meg, hogy a fenyegető tényezők összessége mennyire képes kompromittálni az információs rendszer biztonságát. A potenciál mértékét befolyásolja a támadó szakértelme, a rendelkezésére álló erőforrások és technikai eszközök, valamint motivációja.

A támadási potenciál annál nagyobb:

- minél nagyobb szakértelem birtokában van a támadó identitás,
- minél több erőforrás és technikai eszköz áll rendelkezésére,
- valamint minél motiváltabb (elszántabb) a támadás végrehajtására.

A támadási potenciál mértékére kihatással van, hogy mekkora a támadás végrehajtásához szükséges, illetve a valójában rendelkezésre álló idő aránya, tovább az is, hogy a támadó a rendszerről előzetesen mekkora ismeretanyaggal rendelkezik.

- A kérdéses információs rendszer milyen sérülékenységi pontokkal rendelkezik. Olyan véletlenül, vagy szándékosan létrejövő adminisztratív és technikai hibák és gyengeségek összessége, melyet a támadók kihasználhatnak. A sérülékenységi pontok feltérképezésére három lehetőség van:
- a sérülékenységi pontokat a támadó az információs rendszer előzetes ismerete nélkül kísérli meg azonosítani,
- részleges adatok állnak rendelkezésére,
- illetve a rendszer teljes felépítésére, működési elvére vonatkozó információk, folyamatábrák a birtokában vannak.

Az utóbbi két esetben feltételezhető, hogy a támadó a műveletek előkészítése során akár különböző technikai eszközök, akár humán információszerző források alkalmazásával feltérképezte a sérülékenységi pontokat.

- Milyen adminisztratív és technikai védelmi intézkedéseket milyen minőségben foganatosítottak.

Egy szervezet információs rendszerének biztonságára nagymértékben kihatnak az üzemeltetésükkel kapcsolatos belső utasítások, melyek pontosan megfogalmazzák az információkhoz való hozzáférés, kezelés rendjét, az azokon – szervezeti egységenként – végezhető lehetséges műveleteket, illetve módját és természetesen a jogosult beosztási szinteket. Az adminisztratív szabályzóknak mindig illeszkednie kell a szervezet tevékenységi köréhez és belső struktúrájához, mivel ellenkező esetben a munkafolyamatokban bizonytalanságok, hiányosságok és biztonsági rések jelentkezhetnek, melyek segíthetik a támadót.

A technikai eszközökkel megvalósított védelem során szintén fontos az adminisztratív intézkedések meghozatala, azonban ezek mellett elengedhetetlen a megfelelő, a várható támadási módozatoknak hatékonyan ellenálló technológia és modern eszközök alkalmazása.

INFORMÁCIÓS FOLYAMATOK ÉS A TECHNIKA KAPCSOLATA

Napjainkban az információs folyamatok egyre nagyobb hatékonyságát, a vezetési ciklus gyors körforgását már fejlett infokommunikációs eszközrendszerek, valamint az ezekből összeálló, akár globális kiterjedésű információs infrastruktúrák, érzékelő-észlelő rendszerek biztosítják. Tekintettel, az infokommunikációs hálózatokkal való összefonódásra az információs folyamatokban kezelt információk bizonyos minőségi paraméterei nagyban összefüggnek a kérdéses hálózat adat- és üzembiztonságával, illetve az általa nyújtott szolgáltatások minőségi jellemzőivel. Erre való tekintettel a vezetési ciklus manipulálása – például a ciklusidő növelése – elérhető az információs rendszer alapját jelentő technikai berendezések, illetve az alkalmazott technológia támadása révén is.

Az információs folyamatok hátterében álló infokommunikációs eszközrendszerek alapvetően öt fő tevékenységi területhez kapcsolódnak:

- *információszerzés:* A számítógépes hálózatok, a kommunikációs rendszerek ma már szerves részei az információszerzés folyamatának, mind technikai, mind pedig humán dimenzióban egyaránt. Adatok keletkeznek a különböző érzékelő-észlelő, tájékoztató, navigációs rendszerekben, stb., továbbá a humán forrásból származó információk – különböző technikai eszközök alkalmazása révén – is e szakaszban kerülnek be a vezetési ciklusba. Ebben a szakaszban felmerülhet a különböző információs rendszerek közötti interdependencia is, mivel előfordulhat, hogy egy információs rendszer információszerző képessége részben vagy nagyban összefügg egy másik rendszer információ szolgáltatási kapacitásával, lehetőségével.
- *továbbítás:* Szinte minden információs folyamatra, vezetési ciklusra jellemző, hogy az adatokat nem a megszerzés helyén fogják feldolgozni, illetve a származtatott információk birtokában megint csak máshol fognak dönteni az optimális intézkedésekről, valamint az intézkedések konkrét végrehajtásáról, így a különböző állomások között az információt továbbítani szükséges, mely háttérfunkcióval szemben a különböző szervezetek – alaprendeltetésük függvényében – más-más szintű elvárásokat támasztanak.
- *tárolás:* Ez a funkció az előző ponthoz hasonlóan, azonban attól eltérően, nem a földrajzi eltolódásokat hivatott kiküszöbölni, hanem az időbelieket. Alapvető követelmény, hogy a ciklusban lévő munkafolyamatok egymásutániságából adódó, illetve információtechnológiai és más okokból (például folyamatos gyűjtés vagy későbbi felhasználásból) létrejövő szünetekben az információk ne vesszenek el.
- *feldolgozás:* A modern döntéshozatali folyamatokban már olyan nagy mennyiségű és sokrétű információ van jelen, hogy a számítógépes rendszerek alkalmazása nélkül – melyek az adatokat rendszerezik, összefűzik, keresik – már nem is lehetne hatékony

információfeldolgozást megvalósítani. Egy olyan szervezet életében, mely a vezetési ciklus időperiódusának csökkentésére törekszik, nem engedheti meg, hogy a rendelkezésére álló információk feldolgozását végző rendszereire ne kiemelt figyelemmel tekintsen.

- *megosztás, szolgáltatás:* Az információs folyamat legutolsó fázisa, amikor is a feldolgozott információ különböző technológiai megoldások révén a jogosultsági szinteknek megfelelően eljut a megfelelő döntéshozói, illetve végrehajtói körhöz.

Napjainkban egyre jobban jellemzővé válik, hogy a különböző szervezetek működési költségeik racionalizálása érdekében nem építenek ki saját infokommunikációs infrastruktúrát, hanem azt a piaci szféra szereplőitől, gazdaságossági megfontolások alapján különböző szerződéses viszonyok alapján veszik igénybe. Ez főleg a továbbítás tevékenységköréhez tartozik, de az egyre jobban terjedő felhő-alapú technológiák miatt a szervezetek más tevékenységeket (például adattárolást, adatfeldolgozást) is külső szolgáltatókra bízzák.

Tekintettel arra, hogy a nyers és a feldolgozott információk, adatok fizikailag gyakorlatilag az információs rendszerek alapját jelentő infokommunikációs infrastruktúrákban vannak jelen, így annak műszaki paraméterei, biztonságára vonatkozó tulajdonságai közvetlenül is összefüggésbe hozhatók a benne kezelt információk bizonyos jellemzőivel. Ennek az lehet a következménye, hogy ha egy szervezet minél jobban kiszervezi információs tevékenységét külső szolgáltatók számára, annál kevesebb lehetősége van befolyásolni az érintett tulajdonságokat, illetve annál jobban kiszolgáltatottá válik az infrastruktúra üzemeltetőjének, így nem fogja maradéktalanul ismerni a várható fenyegetettségeket, illetve azok szintjét, amiből adódóan a várható zavarokra sem fog tudni kellően felkészülni.

AZ INFORMÁCIÓ TULAJDONSÁGAI ÉS A LEHETSÉGES TÁMADÁSI MÓDOZATOK KÖZÖTTI ÖSSZEFÜGGÉSEK

A támadó, céljainak függvényében az információs rendszerben kezelt információk különböző tulajdonságainak manipulálásával jelentősen képes befolyásolni a vezetési ciklus különböző állomásainak eredményét, így – az egymásra-épülés jellegéből adódóan – egy generált hiba a ciklus következő állomásán már esetleg hatványozottan jelentkezhet.

A vezetési ciklust kiszolgáló infokommunikációs rendszer sebezhetőségi pontjainak ismeretében a támadó felmérheti, hogy mely tulajdonságok vonatkozásában lehet érdemi lehetősége arra, hogy beavatkozzon az ellenérdekelt fél információs tevékenységébe.

Az információ támadhatósága szempontjából elengedhetetlenül szükséges annak funkcionális jelentését, illetve minőségi követelményeit is megvizsgálni. Az információ analizálása során az alábbi jellemzőket lehet, illetve kell tanulmányozni, melyekből következtetni lehet, annak minőségére, használhatóságára, valamint az információs rendszerben betöltött fontosságára, illetve támadhatóságára [4:12]:

- Időszerűség: Az információt akkor kell szolgáltatni, amikor arra szükség van, azaz a kérdésre adott válasznak a kérdező által megkívánt időtartományon belül kell megérkeznie. E paraméter kapcsán a támadónak – amennyiben az információ rendelkezésre állási és felhasználási helye nem egyezik meg – a továbbítást végző infokommunikációs rendszer manipulációja révén érhet el eredményeket. A kommunikáció akadályozása mindkét irányba kiterjedhet, vagy a kérdés, vagy a válasz ne érjen célba, illetve csak olyan jelentős időveszteséggel, hogy az az információ e tulajdonságával szemben támasztott követelményt már ne elégítse ki, így a döntéshozó nem lesz birtokában minden szükséges információnak. Az infokommunikációs rendszer támadása során az ellenérdekelt fél széles palettáról

választhat, a fizikai pusztítás eszközeitől kezdve, az elektronikai ellentevékenységen át, akár a számítógép-hálózati hadviselés eszközrendszeréig.

- Aktualitás: Az adott identitásról érvényes, naprakész információt kell szolgáltatni, vagyis a válaszadó ne olyan információt szolgáltasson, mely már nem a valós állapotot tükrözi. Az aktualitás tulajdonságnál is hatékonyan használhatók az időszerűségnél vázolt támadási módok, melyek a kommunikációt akadályozzák, azonban ezek itt még kiegészíthetőek olyan módszerekkel, melyek arra irányulnak, hogy az információs rendszer első lépcsőjeként is értelmezhető adatgyűjtő, érzékelő mechanizmusok ne tudjanak rendeltetésszerűen működni, illetve félre legyenek vezetve.
- Időperiódus: Az információ érvényességére vonatkozó időtartam, ami vonatkozhat múltra, jelenre és jövőre. Az információs folyamatok szempontjából rendkívül fontos, hogy az adatok megszerzésének gyakorisága illeszkedjen a leírni kívánt környezeti jellemző változásának gyakoriságával, mivel csak ez garantálja azt, hogy aktuális információ legyen a birtokunkba. A múltra, illetve a jelenre vonatkozó pontos információk segítenek a jövőre vonatkozó tendenciák, becslések minél pontosabb meghatározásában. E jellemző a védekezés során lehet fontos, amennyiben valamelyik egyik félnek van lehetősége és erőforrása ahhoz, hogy környezeti jellemzőit az ellenérdekelt fél időperiódusánál gyorsabban változtassa.
- Elérhetőség: Az a paraméter, mely megmutatja, hogy az információra vonatkozó kérdésre milyen gyorsan és milyen könnyen vagy nehezen szerezhető meg a válasz. A támadó célja e paraméter esetében az, hogy a válasz megszerzésének idejét oly annyira elnyújtsa, hogy mire az a döntéshozóhoz ér, már ne a valóságot tükrözze. Ezt elérheti az információs folyamatok (információszerzés, továbbítás, feldolgozás) lassításával, vagy amennyiben erre lehetősége van, az információgyűjtés tárgyát képező entitás módosításával.
- Megbízhatóság: Az információnak, a benne előforduló hibákból származtatott minőségi jellemzője. A hibamentesség bár minden rendszerben alapkövetelmény, azonban ez nem minden esetben biztosítható, így az információ felhasználása során egyfajta tűréshatárt kell bevezetni, melynek keretein belül fel lehet készülni az esetleges eltérésekre, és azok hatásait kezelni lehet. Egy hatékony információs rendszerben elemezni kell a hibás adatok révén megvalósuló esetleges következményeket is. A megbízhatóság az információ egyik legsarkalatosabb jellemzője, így ez a támadások egyik legfontosabb célja. Az információs megbízhatósága – melyen sok esetben a pontosságot is érthetjük – több ponton is támadható. Az információszerzés folyamatában már a keletkezés szakaszában lehetőség van a megbízhatóságot befolyásolni, mely egyrészt elérhető, a környezeti jellemzők módosításával, hogy az adatgyűjtő-rendszerek ne a valóságot észleljék, másrészt pedig az adatgyűjtő-rendszerek műszaki paramétereinek befolyásolásával is. Megfelelő támadópotenciál birtokában az információs rendszerben kezelt adatok megbízhatósága manipulálható a továbbítás és a tárolás szakaszaiban is. Az adatok, információk módosítása esetén figyelembe kell venni, hogy a túlzott torzítás (dezinformálás) a támadás tényét azonnal leleplezheti.
- Jelentőség: A felhasználó valódi információigényéhez kapcsolódó fogalom, ami a felhasználó számára az információ fontosságát jelzi, melyet becsülni lehet abból, hogy az információ megszerzésére mekkora erőforrásokat szabadítanak fel egy szervezeten belül. Ezen paraméter támadása abszurd módon a megszerezni kívánt információ védelmével érhető, ha az ellenérdekelt felet lehetőségeinkhez mérten elzárjuk az őt érdeklő adatoktól. Ez az elzárás jelentheti azt, hogy védjük saját információinkat, de jelentheti azt is, hogy az ellenérdekelt felet olyan más

információs infrastruktúráktól szigeteljük el (akár a kérdéses struktúra támadásával), ahonnan információk kerülnek át saját rendszerébe. További közvetett támadási mód lehet, ha a szervezetet elvágjuk azoktól az erőforrásoktól, melyeket az információ megszerzésére tudna fordítani.

Teljesség: Fontos szempont, hogy minden információ rendelkezésre álljon a döntéshozatal során. A teljesség problematikájához tartozik az is, hogy ha egy információ egy másik információra hivatkozik, akkor a hivatkozott információnak is elérhetőnek kell lennie. A teljesség hiánya a döntéshozó bizonytalanságát erősíti. Hogy a teljesség a követelményeknek megfeleljen, fontos, hogy minden egyes részinformáció eljusson a döntéshozóhoz. E tulajdonság támadása gyakorlatilag magának az információnak a támadásával egyezik meg, mivel ha a részinformáció bármelyik tulajdonságát lehet támadni, akkor az kihat a teljes információra, ez által fejtve ki a hatást.

- Igazolhatóság: Ugyanarra a kérdéskörre különböző helyekről, válaszadóktól, információs csatornákból származó válaszok mennyiben egyeznek meg, illetve mennyire térnek el, ami az információk ellenőrzöttségére, felhasználhatóságára vonatkozhatnak. Az igazolhatóság nem megfelelő szintje szintén a döntéshozó bizonytalanságát növeli. Az igazolhatóság a teljességhez hasonlóan egy olyan paraméter, mely egy párhuzamosan futó, gyakorlatilag azzal megegyező információs folyamattól függ, így támadása magának az információnak a támadásával egyezik meg.
- Bizalmasság: Az információ e tulajdonsága azt hivatott biztosítani, hogy ha az ellenérdekelt fél már részben eredményesen támadta az információs rendszer valamely folyamatát (például továbbítást, tárolást) az információ akkor is csak az arra felhatalmazottak számára legyen elérhető, érthető. A támadó, megszerezve a titkosított információkat, megfelelő szakértelem és elegendő számítási kapacitás birtokában kriptográfiai módszerek segítségével juthat hozzá a kívánt információhoz.

KONKLÚZIÓ

Az információs társadalom kapcsán gyakorlatilag törvényszerűségként kijelenthető, hogy az információt felhasználó környezetében szinte mindig létezik egy olyan másik ellenérdekelt entitás (személy, hadsereg, terrorcsoport, szervezet, gazdasági társaság), mely arra törekszik, hogy a felhasználó információs folyamataiba beavatkozva a felhasználót az optimálistól eltérő döntésre kényszerítse, így szerezve előnyt magának az ellenérdekelt fél.

Elérni kívánt cél az lehet, hogy az ellenérdekelt fél a döntési ciklusához szükséges információkhoz ne jusson hozzá (elérhetőség), ne a szükséges időben kapja meg azokat (időszerűség és aktualitás), vagy a kapott információk pontatlanok legyenek (pontosság) , továbbá, hogy ne legyenek ellenőrizhetők (megbízhatóság, igazolhatóság), stb.. Amennyiben az információs rendszerben kezelt információk ellen alkalmazott eljárás, vagy eljárások összessége minél több minőségi jellemzőt érint, annál eredményesebbnek tekinthető az információs támadás.

Egy információs művelet előkészítése során a támadónak objektíven fel kell mérnie, hogy mekkora támadási potenciál birtokában van. Az elérni kívánt cél függvényében meg kell határoznia, hogy azt a rendszerben kezelt információk, mely tulajdonságainak manipulálásával érheti el leghatékonyabban. Az információs rendszer üzemeltetőjének szempontjából pedig azt kell meghatározni, hogy melyek azok a tulajdonságok, melyek a működés szempontjából kiemelten érzékenyek a támadásra, és melyek védelmét akár külön erőforrások bevonásával is erősítenie kell. Továbbá azt is célszerű felmérni egy szervezetnek,

hogy az információs folyamatokba kívülről bevont, vagy épp kiszervezett – más szervezetek által biztosított, és más elvek, módok alapján védett – folyamatok esetleges támadása mennyiben érintheti, milyen kihatással lehet a saját rendszerének működésére.

Felhasznált irodalom

[1] Wikipedia - http://hu.wikipedia.org/wiki/Inform%C3%A1ci%C3%B3, letöltve: 2011. május 20.

[2] Ujváriné dr. Melich Katalin - A gazdasági informatika alapjai, Perfekt Zrt. 2008., ISBN 978-963-394-734-0

[3] Haig Zsolt, Várhegyi István - Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest 2008., ISBN 9633273919

[4] Papp Zoltán - Kritikus információs infrastruktúrák elleni lehetséges támadások (Diplomamunka), ZMNE-BJKMK, Budapest 2009.,

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Papp Zoltán
pappz.szeged@gmail.hu

IRÁNYÍTOTT ENERGIÁJÚ FEGYVEREK VESZÉLYEI A KOMMUNIKÁCIÓS HÁLÓZATOKRA

Absztrakt

Az információs társadalmat átszövő infokommunikációs hálózatok folyamatos rendelkezésre állása kiemelt fontosságú, mivel az azok által nyújtott szolgáltatások hozzájárulnak a társadalom, az egyének, illetve a gazdaság szereplőinek egymás közötti kapcsolatainak létrejöttéhez, fenntartásához, valamint a védelmi szféra, az államigazgatás működéséhez. A kérdéses rendszerek biztonságára azonban veszélyt jelenthetnek a különböző motivációkkal rendelkező támadók, akik különböző típusú és fejlettségű elektromágneses fegyverekkel hatékonyan képesek pusztítani a kérdéses hálózat elemeit.

The constant availability of infocommunication networks intertwined with modern information society is of utmost importance, since their services contribute to the establishment and maintenance of relationships among the society, the individuals and the economic actors as well as the operation of the defense sphere and public administration. The security of the systems in question may be threatened by attackers with various motives who can efficiently destroy the elements of such networks by applying various types of radio frequency weapons.

Kulcsszavak: *infokommunikációs hálózatok, infokommunikációs hálózatok pusztítása, rádiófrekvenciás fegyverek, információs társadalom ~ infocommunication networks, destroying of infocommunication networks, radio frequency weapons, information society*

BEVEZETŐ

Napjaink információs társadalmának működéséhez elengedhetetlen az, hogy az infokommunikációs hálózatok technikai eszközei, berendezései megbízhatóan üzemeljenek, mivel ezek biztosítják az egyének, illetve a különböző szervezetek információs folyamatainak a folytonosságát.

A modern félvezető elektronika már lehetővé teszi, hogy ezekbe a hálózatokba beépítésre kerülő eszközök egyre kisebb méretűek legyenek, és egyre nagyobb alkatrész-sűrűségű integrált áramkörökből épüljenek fel, melyek egyre nagyobb hatékonyságot biztosítanak. Az egyre nagyobb műszaki és gazdasági hatékonyság érdekében az infokommunikációs hálózatokat üzemeltető szolgáltatók az elvárt műszaki paraméterekhez pontosan illeszkedő alkatrészeket szereznek be, azok azonban szélsőséges terhelésekre, extrém környezeti viszonyokra nincsenek méretezve. Az eszközök méretének csökkenésének egyik következménye az, hogy – a miniatürizálást lehetővé tevő technológia jellegéből adódóan – csökken a rétegvastagságuk, ami miatt érzékenyebbek válnak a túlfeszültségre. Amennyiben az ilyen berendezések környezetében intenzív elektromágneses térerősség változás történik, akkor a belső vezetékhálózatokon kritikus nagyságú feszültség indukálódhat, ami ennek következtében a félvezető rétegek között átütést okozhat. A villamos átütések a félvezetőkben javíthatatlan károkat idéznek elő.

A fenti jelenséget kihasználva az infokommunikációs hálózatok berendezései hatékonyan rombolhatók lehetnek a különböző elven működő rádiófrekvenciás fegyverekkel. E fegyvertípusok képesek lennének egy adott földrajzi területen kiiktatni a kérdéses rendszereket, illetve minden hasonló elektronikai eszközt, valamint az általuk nyújtott szolgáltatásokat, melyek helyreállítása a nagy költség mellett sok időt is követel.

A veszélyeztetett eszközök

A bázisállomások technológiájának elméletét az amerikai Bell Labs mérnökei már 1947-ben kifejlesztették az AT&T telefontársaságnál, és folyamatosan fejlődik napjainkban is. A bázisállomások kifejlesztésével párhuzamosan hozták létre a rádiótelefonok nulladik (0G) generációját is, azonban ezeket a szakirodalom nem sorolja be a mobiltelefonok közé, mivel még nem voltak képesek a kommunikációs csatorna frekvenciájának automatikus váltására, a beszélgetés csak egy bázisállomáson (cella) keresztül folyt, ami azt jelentette, hogy a beszélgetés ideje alatt folyamatosan a kérdéses bázisállomás hatósugarában kellett tartózkodni. A hívásátadás – a mozgásból adódó cellaváltás lehetőségének – problematikája az 1970-es években oldódott meg, és így vált a rádiótelefon mobiltelefonná. Kezdetekben ezeket a készülékek robosztus méretükből adódóan főleg gépkocsikban alkalmazták, de az elektronika fejlődése révén az 1980-as évektől már kézi kivitelben is elérhetőek lettek, és mivel előállításuk viszonylag olcsó, könnyen fejleszthetők, ezért a mobiltelefon-hálózatok rohamos gyorsasággal terjedtek el a világban.

Napjainkban a mobiltelefonok, illetve az egyéb mobilkommunikációs berendezések már a legelterjedtebben és a leggyakrabban használt eszközeink közé tartoznak. A készülékekbe integrált, illetve általuk a kibernetikus térben elérhető szolgáltatásokra az információs társadalom tagjai, valamint gazdasági, közigazgatási és rendészeti szervezetei életük és működésük során fontosabb és kevésbé fontosabb részterületén egyaránt számítanak. Az információs társadalom egyre növekvő igényei miatt a városok – ahol az információ felhasználói legnagyobb létszámban vannak jelen – egyre sűrűbben be lesznek hálózva az infokommunikációs hálózatok eszközeivel.

A nagyfokú fejlettség az infokommunikációs infrastruktúrákban egyben kiszolgáltatottá is teszi a társadalmat, mivel a hálózatokban keletkezett véletlen vagy épp szándékosan előidézett zavarok azonnal a társadalom széles körét érintik, és más infrastruktúrákba is átgyűrűznek, így tovább szélesítve a negatív hatások körét. A jelenség, miszerint az információs társadalom számos folyamata a mobilkommunikációs eszközök révén is elérhető kibernetikus térben zajlik, értelemszerűen elhozta azt a következményt, hogy a különböző indíttatású támadók igyekeznek hozzáférni, befolyásolni az infokommunikációs hálózatokban kezelt információkat, adatokat, illetve a rendszer szolgáltatásaiban zavarokat okozni, ezáltal másodlagos következmény formájában érni el a kívánt célt.

Az infokommunikációs rendszerekben zavart okozni kívánó támadónak számos eszköz és módszer állhat rendelkezésére, hogy célját elérje. Az érintett rendszerekben kezelt információ bizalmasságát, titkosságát számos módszerrel (például titkosítással) védik, így az információ tartalma ellen indított támadások nagy szakértelmet, modern eszközparkot és számítási kapacitást igényelnek. Azokban az esetekben, amikor a támadó nem a rendszerekben kezelt információ tartalmát kívánja megváltoztatni, manipulálni, hanem csak magának az információnak az elérhetőségét, hozzáférhetőségét akarja akadályozni, kevésbé szofisztikáltabb lehetőségek is rendelkezésére állnak. A szóba kerülhető módszerek nagyban függnek a támadó támadási potenciáljától, mely azt mutatja meg, hogy a fenyegető tényezők összessége mennyire képes kompromittálni az információs rendszer biztonságát. A potenciál mértékét befolyásolja a támadó szakértelme, a rendelkezésére álló erőforrások és technikai eszközök, valamint motivációja.

Elektromágneses fegyverek

A fizikai pusztítás eszközeivel a mobiltelefon-technológia sajátosságaiból adódóan egy földrajzi területen egy időben elérhető, szétszórtan elhelyezkedő bázisállomások lerombolása nehezen kivitelezhető. További nehézség, hogy a felhasználóknál lévő mobil kommunikációs eszközök – nagy számuk, szétszórt és rejtettnek tekinthető elhelyezkedésük révén – e módszerrel egy időben nem iktathatók ki.

Egy kérdéses területen a mobil kommunikációs rendszerek elemei azonban nagy hatékonysággal pusztíthatók elektromágneses fegyverekkel. A nagy energiájú rádiófrekvenciás sugarak alkalmazásának célja a felvezetők károsítása, a mikroáramkörök (processzorok, memóriák) túlterhelése, a villamos alkatrészek szigeteléseinek átütése és ezáltal az elektronikai eszközök tönkretétele. [1] Az elektromágneses impulzusok elleni védekezésnek csupán gazdasági korlátai vannak, a berendezések gyártóinak – elsődlegesen a megrendelők gazdaságossági szempontjainak tükrében – kell azt eldönteniük, hogy mit és mi ellen védjenek.

A nagy erejű professzionális fegyverek elvileg csak a hadseregek eszköztárában lelhetők fel, de léteznek kisebb erejű, készre gyártott, sőt elvileg megvásárolható változatok is:

1. ábra. EMP mikrohullámú sütőből
(forrás: www.fegyverlabor.hu)

2. ábra. Az Internetről rendelhető EMP eszközök (forrás: http://www.amazing1.com/emp.htm)

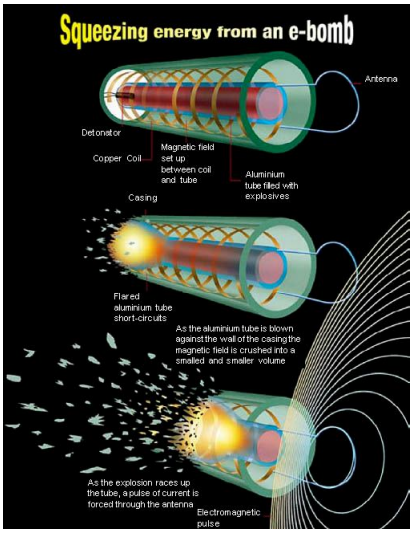
Ugyanakkor ezek az eszközök kereskedelemi forgalomban kapható alkatrészekből is összeállíthatók, melyeket a támadók (terroristák) könnyedén felhasználhatnak céljaik elérése érdekében. Felhasználható az egyszerű mikrohullámú sütő magnetronjától kezdve, régi televíziós készülékek feltöltött képcsövéig, a fényképezőgépek nagyteljesítményű vakujáig minden.

Ezen eszközök működési elve csaknem azonos. Feltölteni egy energiatárolót, ami akár egy egyszerű fényképezőgép vakujában található kondenzátor is lehet, és adott időben és helyen a lehető legrövidebb idő alatt kisütni. [1]

A nagy energiájú rádiófrekvenciás fegyverek közül az elektromágneses impulzusbomba (EMP) a leghatékonyabb, melynek vannak nukleáris (NEMP) és nem nukleáris (NNEMP) alapú implementációi is. A hidegháború elmúltával a nukleáris alapú elektromágneses impulzus fegyverek háttérbe szorultak, de a nem nukleáris alapú eszközök fejlesztése töretlen. A NNEMP fegyverek lényegesen szűkebb tartományban (kisebb hatóerővel, kisebb hatókörrel) működnek, azonban másodlagos hatásaik (például radioaktivitás) nincsenek, vagy elhanyagolhatók, így alkalmazhatók precíziós csapásokat igénylő műveletekben. A nem nukleáris elektromágneses impulzusfegyverek többféle megoldást használnak a nagy energiájú elektromágneses lökéshullám előállítására.

A rádióhullámok fegyvertechnikai alkalmazása esetén meg lehet különböztetni:

- impulzusüzemű, és
- periodikusan rádióhullámokat sugárzó rádiófrekvenciás fegyvereket.



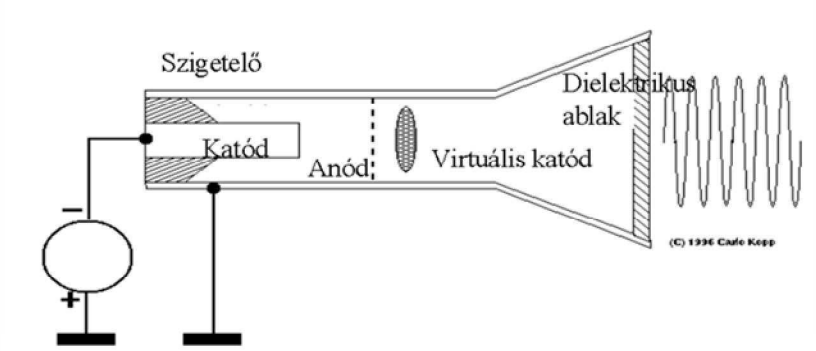
3. ábra. Az E-bomba működése (forrás: www.countdown.org/end/pix/ebomb.jpg)

Az ilyen fegyverek három részből állnak: egy energiaforrásból, melyek a mikrohullámok generálásához szükséges nagy mennyiségű statikus energiát tárolják, egy mikrohullámot generáló eszközből, és egy antennából, mely a kívánt irányba sugározza a generált mikrohullámokat. Az energiát tároló eszköz lehet Marx generátor vagy fluxus kompressziós generátor. A fluxus kompressziós generátor több MJ energiájú elektromos energiát képes előállítani rövid (10-100 μs) ideig. A viszonylag kisméretű eszköz több MW impulzusteljesítményű energiaforrásnak számít. Működési elve azon alapul, hogy egy induktív energiatárolóban tárolt elektromágneses energiát robbantással, a tekercs meneteinek rövidre zárásával áramimpulzussá alakítja. Mivel az impulzusbombában alkalmazott fluxus kompressziós generátort a robbanótöltet hozza működésbe, ennek következtében az eszköz megsemmisül. [2]

A Marx generátor számos kaszkádba kapcsolt kondenzátort alkalmaz, melyek mindegyike párhuzamosan kapcsolódik a töltőrendszerre, így ugyanarra a feszültségre van feltöltve. A kondenzátorok szikraközökkel vannak elválasztva egymástól. A generátor elsütésekor a szikraközök begyújtanak és az addig párhuzamosan kapcsolt kapacitásokat a kimenet felől tekintve sorba kapcsolják, így nagyfeszültséget generálnak ezzel. Az impulzus időtartama 4-100 ns, de ez idő alatt több száz A nagyságú áram folyhat az elektromágneses hullámot gerjesztő eszközben. [1]

A folytonos, periodikus jel előállítására alkalmas eszközök közül legelterjedtebb a virtuális katódú oszcillátor, amely a rádiófrekvenciás fegyverek abba a csoportjába tartozik, amely – a fluxus kompressziós generátort használó fegyverekkel ellentétben – többször is felhasználható. [3]

4. ábra. Vircator
(forrás: www.amazing1.com/emp.htm)



5. ábra. Elvi felépítése
(forrás: www.amazing1.com/emp.htm)

Az NNEMP fegyverek talán legveszélyesebb tulajdonsága az, hogy viszonylag távolról is alkalmazhatóak, a támadásra való felkészülés nehezen észlelhető, a támadásnak pedig külső jele nincs. A sikertelen támadásnak nyoma nem marad, egy sikeres támadásnál pedig a megtámadott kommunikációs rendszerek üzemeltetői és felhasználói csak a hatást, azaz eszközeik tönkremenetelét érzékelik.

ÖSSZEGZÉS

Az információs társadalom modern nagyvárosaiban az infokommunikációs hálózatok eszközei a speciális környezeti jellemzőkből adódóan nagy sűrűséggel vannak telepítve, így egy elektromágneses támadás nagyszámú berendezésben tehet kárt, melyek helyreállítási költségei jelentősek lehetnek. A fizikai károkon túl további veszteségek jelentkezhetnek a kieső szolgáltatások révén, valamint szervezetek esetében számolni kell a jelentkező bizalomvesztéssel is.

Ilyen típusú fegyverek alkalmazásának lehetősége egyre valószínűbb, mivel a megalkotásukhoz szükséges tervrajzok megtalálhatók az Interneten, a szükséges alkatrészek kereskedelmi forgalomban beszerezhetők és kisebb gyakorlattal házilag is megalkothatók, így pedig a potenciális támadók köre – túl a hadseregeken, terroristákon – lényegesen kiszélesedhet. A kevésbé elszánt, kisebb támadó potenciállal rendelkező támadók részéről nem az egyszer használható, robbanással működésbe hozható eszközök alkalmazására lehet elsősorban számítani, hanem a többször felhasználható – bár kisebb hatótávolságú és hatékonyságú – berendezések használata merülhet fel.

Prognosztizálható, hogy az információs infrastruktúrák üzemeltetőinek, illetve az ő hálózatukon kiemelt jelentőségű szolgáltatásokat nyújtó felhasználóknak a fontosabb elektronikus eszközeik védelmének szintjének emelésére az elkövetkezendő időszakban fokozott figyelmet kell fordítaniuk.

Felhasznált irodalom

[1] Dr. Kovács Tibor - A terroristák láthatatlan fegyverei (ZMNE Terrorizmus Konferencia 2006.)

[2] Csuka Antal, Előházi János - Irányított energiájú fegyverek és veszélyeik a számítógépes rendszerekre (Hadmérnök, III. Évfolyam 3. szám. 2008. szeptember, ISSN 1788-1919);

[3] Dr. Ványa László - Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre (Doktori (PhD) értekezés, ZMNE, Budapest, 2001.)

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Szabó András
szaboandras@mil.hu

PREVENTÍV HÁLÓZATVÉDELMI RENDSZEREK ALKALMAZÁSI LEHETŐSÉGEI A TÁMADÁSOK DETEKTÁLÁSÁRA, VALAMINT A MÓDSZEREK ELEMZÉSÉRE
I. RÉSZ

Absztrakt

Elméleti kutatásokat, összehasonlítások, valamint kísérletek segítségével vizsgáltam a hálózatvédelmi módszerek (tűzfal, IDS / IPS, proxy szabályok) hatásfokának javítási lehetőségeit. A bemutatott módszerek az eddig ismeretlen támadási minták felismerésére és gyűjtésére alapulva végzik a biztonságot támogató tevékenységüket. Összefoglaltam a különböző honeypot típusokat, valamint többféle csoportosítás alapján értékeltem ezen rendszerek előnyeit, valamint hátrányait.

In my survey I explored, compared, and demonstrated methods to increase the efficiency of the network defense system (firewall and IDS/IPS, proxy rule set). These methods support the detection and collection of unknown malicious codes, and attack vectors. I summarized the different honeypot types as well as I categorized them based on different methods. I compared the pros and contras of these honeypot types.

***Kulcsszavak**: preventív, IT biztonság, kiber, hálózatvédelem, honeypot, megtévesztés, ~ preventive, IT security, cyber, network security, honeypot, deception*

A HÁLÓZATVÉDELEM KORSZERŰ MÓDSZEREI

A hálózatvédelmi képességek kutatása során gyakran találkozunk más tudományterületek tapasztalatainak felhasználásával: a számítógépes vírusok kutatói párhuzamot vontak saját kutatásaik és a biológia eredményei között (Járványtan, Immunológia stb.), a mesterséges intelligencia kutatás az agy működésének feltárásával párhuzamosan fejlődik stb. Így nem meglepő, hogy a hadtudomány eredményei, módszerei is bizonyos mértékben alkalmazhatóak a virtuális tér védelmére.

A világtörténelem nagy stratégái, mindig is helyes logikai döntéseikre (a kívánt hatás eléréséhez szükséges mennyiségű, minőségű erők és eszközök, a megfelelő időben és helyen történő alkalmazása)[1], mint az erők megfontolatlan bevetésére alapozták sikerüket.

Az alkalmazott taktika függvénye, hogy a kívánt hatás eléréséhez milyen tekintetben kell fölénnyel rendelkeznünk az ellenséggel szemben[2]. Ezek az előnyök, hatásnövelő faktorok csak akkor érvényesülnek, ha a taktika, stratégia szintjén sikerül követni a meghatározott terveket, elgondolásokat. Amennyiben az ellenség ki tudja kényszeríteni, hogy a saját taktikáját kövessük, az ő hatásnövelő faktorai fognak érvényesülnek. Ennek folytán ismernünk kell eszközeit, és céljait, hogy azok ellenünk történő alkalmazását megelőzzük, hatásaik ellen védekezni tudjunk.

Ezen elméleti eszmefuttatás alkalmazható a kiberhadviselésben, hiszen naprakésznek kell lennünk az ellenséges entitás[3] taktikái és "támadási trendjei" terén annak érdekében, hogy felkészüljünk az általa gerjesztett fenyegetésre, és eredményesen vívjuk meg defenzív csatánkat a virtuális térben.

Fenyegetésekkel mindig is számolnunk kell, amennyiben elvárásokat[4] támasztunk az üzemelő informatikai hálózattal, rendszerrel szemben. Az informatikai biztonsági kontrollok segítenek felkészülni a rendszer „nyugalmi”, ideális állapotát megzavaró helyzetekre, az incidens teljes életciklusa (kialakulása, észlelése, kezelése) alatt. Ezt a célt csak abban az esetben tudja elérni, amennyiben feltételezzük és modellezzük a támadó szándékot, valamint ismerjük a támadó céljait, eszközeit.

Az informatikai védelmi eljárások az incidensre adott válasz alapján, az idősikon csoportosíthatóak [1.]:

- Preventív,
- Korrektív, vagy Reaktív,

---

[1] Lásd:pl.: ie. 480 - Thermopülai csata, ie. 202 - Zamai csata

[2] Erre számos példát találunk a történelemben:
a kiképzésbeli fölény, mellyel például a német Fallschirmjäger ejtőernyős csapatok rendelkeztek,
a mozgékonyság, dinamika okozta előny, melyre a német villámháborús harckocsi-ékek és vadászbombázók kombinált alkalmazása példa,
a mindent elsöprő tüzérség ereje: a katyusa, a szovjet rakéta-sorozatvetővel végrehajtott tűzcsapások,
a hírszerzés sikerei: a német tengeralattjáró hadviselés kudarcai részben az Enigma algoritmusának feltörése okozta,
a nagytávolságú fegyverek elrettentő ereje – A németek V1 és V2 rakétákkal végrehajtott, nagytávolságú csapásmérő műveletei,
a terep ismeretének kamatoztatása – a Finn halogató harc sikerei a szovjet offenzíva idején, vagy a váratlan támadás, meglepetés ereje - például a SAS Észak Afrikai bevetései során.

[3] Legyen az organikus: kiberbűnöző, hacker, cracker vagy mesterséges entitás: kártékony kód.

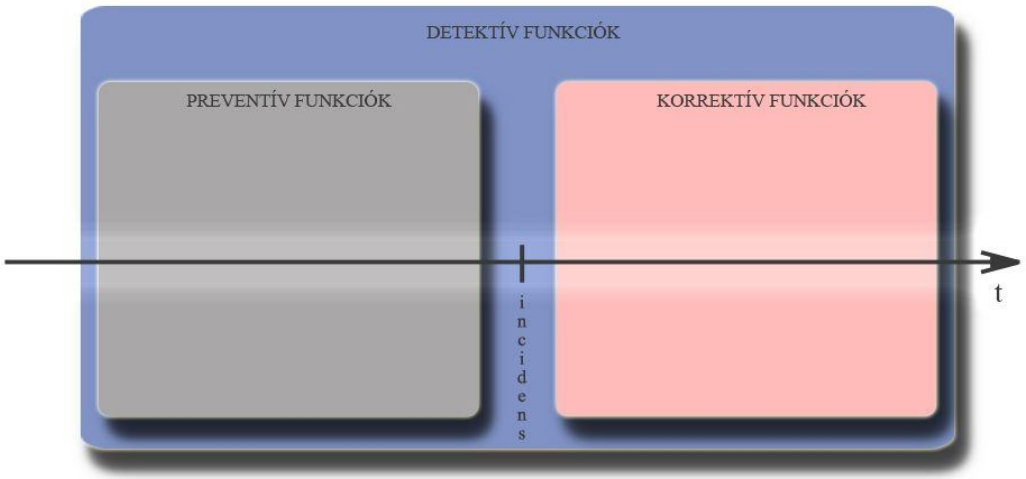
[4] Legyen az üzembiztonsági (szolgáltatás minősége, rendelkezésre állás), vagy információbiztonsági jellegű (bizalmasság, sértetlenség, rendelkezésre állás, hitelesesség, elszámolhatóság)

- Detektív tevékenységekre.

A *preventív funkciók* biztosítják a biztonsági incidensek megelőzését, a támadások alapjául szolgáló sérülékenységek megszüntetését, azok kihasználásának akadályozását.

A korrektív, *reaktív funkciók* a támadások bekövetkezte után aktivizálódnak, és próbálják megszüntetik a biztonsági incidens kiváltó okát, minimalizálják a károkat.

A *detektív funkciók* a támadások nyomainak gyűjtését, hiteles rögzítését, és megjelenítését végzik az incidens bekövetkezése előtt, alatt és után.



1. ábra A biztonsági kontrollok ábrázolása az incidens idősíkján

Az informatikai biztonsági alrendszerei (tűzfal, vírusvédelem, jogosultság kezelés, behatolás detektálás) ezeknek a funkcióknak egyikébe, vagy akár egyszerre többe is besorolható (pl.: a tűzfal alrendszer egyrészt a szabályrendszere alapján blokkolja a támadás, másrészt naplózza a próbálkozást).

A támadásokat klasszikusan kétféle módszerrel lehet detektálni [2][3][4]:

- ha ismerjük a támadást, a generált hálózati forgalom alapján mintákat (~*signature*) hozhatunk létre, a detektálás ekkor mintaillesztéssel zajlik (*knowledge-based IDS vagy signature based detection*);
- ha ismerjük a védett hálózat jellemzőit (forgalom típusa, eloszlása, végpontok, hálózati szolgáltatások), felállítható egy alapérték (~baseline), az ettől bizonyos mértékben történő eltérés indikálja a támadást, ez az úgynevezett anomália alapú detektálás (*behavioral-based* IDS vagy *anomaly based detection*).

A napjainkban alkalmazott határvédelmi eszközök általában mindkét eljárást alkalmazzák. Azonban hátrányuk, a magas hibaarány (a tévesen támadásnak felismert legitim forgalom, valamint a fel nem ismert támadások). Ezt a hibaarányt javíthatjuk plusz védelmi intézkedések bevezetésével, támogató tevékenységek alkalmazásával. Amennyiben ismert a kontroll hiányossága, az eszközök finomhangolásainak segítségével azok hatékonysága növelhető (a gyári beállításokat, vagy az úgynevezett bevált gyakorlatokat kiegészítik, illesztik a védett hálózathoz, a felhasználás jellegéhez). A következőekben egy ilyen támogató tevékenységet mutatok be, mely elősegíti a hálózatvédelmi eszközök kalibrációját, testre szabását.

Jelen dolgozat témája szorosan kapcsolódik Kassai Károly mk. ezredes úr doktori értekezésében [5] felvázolt, NATO- és nemzeti információvédelmi fejlesztési igényekhez.

HONEYPOT (~ MÉZES CSUPOR, CSALI RENDSZEREK)

Az elektronikai hadviselésben régóta alkalmazott ellentevékenység a megtévesztő célok („decoy", „chaff") alkalmazása, mely segítségével az ellenséges felderítő lokátorok, légvédelemi rakéták téveszthetőek meg, hamis céljelek generálásával. Ennek a védelmi tevékenységnek a logikáját követve, az informatikai hálózatok védelme során is hatékonyan alkalmazható a támadó megtévesztésére szolgáló csali rendszerek (*bait system*).

A „csali" (~ honeypot) olyan számítógépes rendszer, mely hálózati szolgáltatások, erőforrások, forgalmak szimulálása segítségével (valós erőforrások, információk) kifejezetten a szándékos támadások detektálására szolgál [6]. A támadási kísérletek, a sikeres támadások és a behatolások eszközeiről (támadási vektorok, malware-ek, exploit-ok) rögzítése mellett az elkövető szándékairól és a valós rendszer sérülékenységeiről is információval szolgál.

Ezen rendszerek (un.: produktív rendszer) a valós rendszerektől függetlenül, azokat nem akadályozva, és nem kompromittálva képesek detektálni a támadási szándékot, rögzíteni a támadási módszert, és a támadó tevékenységét [6].

Sokféle típusa és fajtája létezik, a hálózati topológiába történő elhelyezésére is számos módszer létezik, azonban az alábbiakban mind megegyeznek:

- céljuk a támadás detektálása (a módszer, az elkövető és a kiváltott hatás);
- a valós rendszerek tulajdonságait szimulálják;
- az automatizáltság mértékének függvényében intenzív felügyeletet, humán interakciót igényelnek;
- védelmi technológiák, és működési rendszabályok segítségével megakadályozzák a csali rendszer további támadásokra történő felhasználását (~kompromittálását).

A Csali rendszerek feladat szempontjából megközelítve lehetnek:

- kutatási célú (pl.:malware-ek, exploit-ok gyűjtése);
- védelmi célú (támadási kísérlet detektálása, a nyomok rögzítése).

A kutatási célú csapda az emulált platformok processzor architektúrájában, az operációs rendszer, szolgáltatások és frissítési szintek tekintetében széles palettát kell kínálnia, annak érdekében, hogy a minél több támadás irányuljon ellenük.

A védelmi célúak elsősorban a védett hálózat jellegzetességeit emulálják, minél inkább elmosva a valós és a produktum rendszerek közti különbségeket (feltűnő lenne, egy vállalati környezetben több, különböző patch-elési szintű, eltérő architektúrájú és verziójú operációs rendszer).

A védelmi célú honeypotok módszer alapján csoportosítóak a következő típusokra:

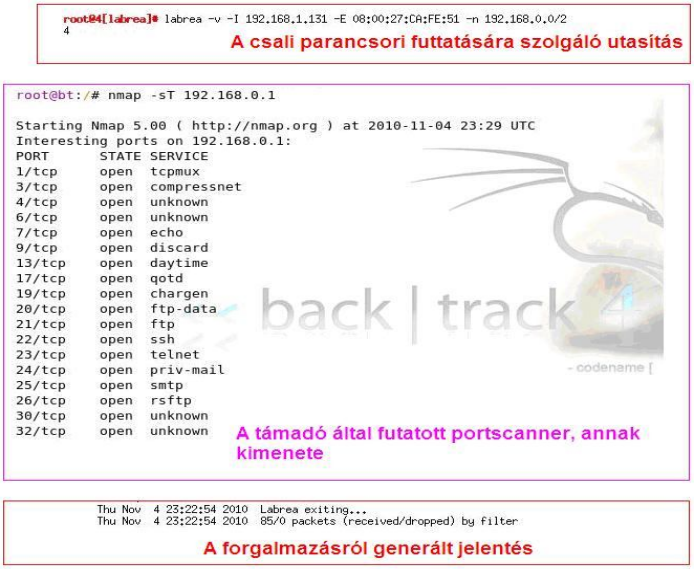
- „Szurokcsapda „ (~Tarpit);
- Forgalom-átirányító (Redirector);
- Internet szimulátor (Internet Simulation Environment).

A tarpit-ek célja a támadó lekötése, a DoS, DDoS támadások, az automatizáltan terjedő kártékony kódok terjedési sebességének csökkentése, melyet hamis célpontok imitálásával, valamint a válaszidő maximalizálásával[5] ér el.

Az alábbiakban összefoglaltam a szurokcsapdákban alkalmazható módszereket:

- IP címtartomány növelése (nem létező címekkel);
- hamis DNS bejegyzések;
- hamis adatkapcsolati- (CDP, ARP, RARP, Ethernet), hálózati (pl.:DHCP),valamint forgalomirányító hirdetések (pl.:RIP, OSPF, BGP);
- TCP ablak méretének 0 értéken tartása;
- TCP deszinkronizáció (hibás szekvenciaszám küldése);
- IP Csomagdarabolás[6];
- hibás FCS, CRC értékek;
- csomagismétlés kérése;
- késleltetés (delay, round trip time - RTT) növelése;
- hozzáférési listák (ACL - Access Control List) segítségével a bejövő/kimenő forgalom korlátozása (konkurens TCP kapcsolatok száma, sávszélesség stb.).

Az alábbi képen [2. ÁBRA] demonstrálom, a *labrea* honeypot alkalmazását, mely működése során a népszerű *nmap*[7] port scanner-t téveszti meg, egy „C" osztályú IP címtartomány összes kliensének emulálásával[8]. Az ábrán csupán egyetlen végpont nyitott portjainak ellenőrzését mutatom be az átláthatóság érdekében, azonban a végrehajtott tesztek során megvizsgáltam az összes emulált végpontot, melyek eltérő nyitott port kombinációkkal „tévesztettek meg".



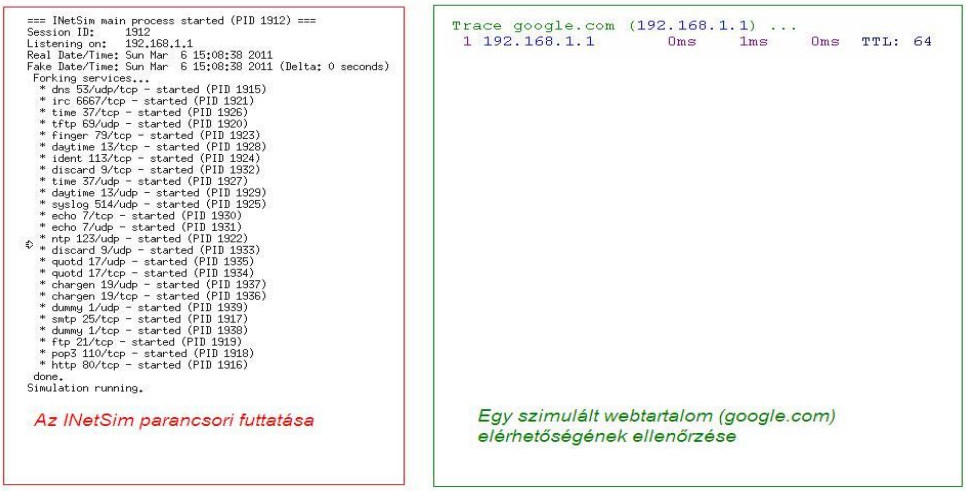
2. ábra A Labrea honeypot által megtévesztett nmap portscanner

[5] Erre a típusra példa a Labrea és a Jackpot nevű nyilvános forráskódú alkalmazás
[6] Pl.:a fragroute, fragrouter eszközök segítségével (lásd részletesen: http://monkey.org/~dugsong/fragroute/)
[7] Ingyenesen letölthető különböző operációs rendszerre a http://nmap.org/ oldalról
[8] A kérésekre adott differenciált válaszok érzékelhetőek a csomag késletetés változásával, és a nyitott portok váltakozásával

A redirector olyan rendszer, melyek a támadás érzékelése esetén a kapcsolódási kísérletet a honeypot irányába továbbítja, gyakorlatilag egy behatolás detektálási feladatkörrel kiegészített forgalomelosztó (Load Balancer). Ilyenre példa a Bait 'N' Switch Honeypot[7] rendszer.

A korszerű kártékony kódok aktivizációjuk (parancs-csatorna kiépítése, kártékony kód letöltése, hálózati felderítés és sérülékenység vizsgálat) előtt gyakran ellenőrzik a hálózati kapcsolat meglétét, az Internet elérést, azonban megfelelő konfiguráció mellett ezek megtévesztése is lehetséges. Az Internet szimulátor a kártékony kódok megtévesztésének gyakran alkalmazott eszköze, működése során a kérésre (DNS lekérdezések, http tartalmak, IRC[9] kapcsolatok) hamis válaszokat ad. Ennek segítségével a kártékony tartalmat publikáló weblapok, botnet vezérlők IP címei azonosíthatóak.

Az alábbi, laborkörnyezetben készített képernyőképeken [3. és 4. ÁBRA] jól látható, hogy a kliens a kéréseire *(trace google.com*, *blabla.com* oldal megnyitása) a szimulátor képes volt válaszokat generálni, tartalmat szolgáltatni.



3. ábra Az InetSim működésének ellenőrzése I.

```
03/08/11 20:29:36 Browsing http://blabla.com/
Fetching http://blabla.com/ ...
GET / HTTP/1.1
Host: blabla.com
Connection: close
User-Agent: Sam Spade 1.14

HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Connection: Close
Content-Length: 258
Content-Type: text/html
Date: Tue, 08 Mar 2011 19:29:34 GMT

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

4. ábra Az InetSim működésének ellenőrzése II.

[9] A botnetek vezérlésének gyakran alkalmazott eszköze (a http kérések/válaszok mellett), az uralom alá vont végpontok egy chat szolgáltatáson keresztül kapják utasításaikat.

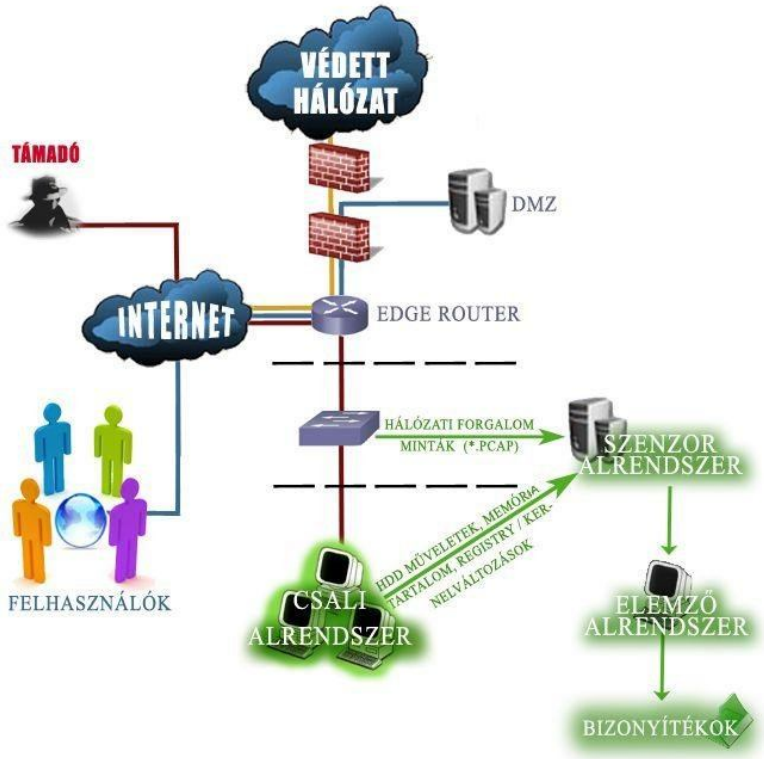
A szimuláció alapbeállítások melletti futtatásáról készültek a fenti képernyőképek. A szolgáltatott tartalom hamis volta egyértelműen detektálható ezek alapján (pl.: a 4.ÁBRA, a HTML kódban található szöveges információ alapján). Azonban az olyan, elsősorban a támadók által használt eszközzel, mint a Social-Engineer Toolkit (SET)[10] alkalmazásával, képesek vagyunk bármely weblap tartalmát klónozni[11], valamint azt lokálisan szolgáltatni.

A honeypot típusától (kutató vagy védelmi) függetlenül felépítésükben felismerhetünk azonos vonásokat, mely jegyeket az egyedi implementációk, speciális típusok sem nélkülözhetnek.

A HONEYPOT RENDSZEREK FELÉPÍTÉSE

1. „Csali" alrendszer (valós vagy emulált szolgáltatás, virtuális számítógép)
2. Szenzor alrendszer (forgalom és tevékenység rögzítése)
3. Elemző alrendszer (a nyomok elemzésére és megjelenítésére szolgál)

Honeypot hatékonysága a „csali" valósághűségétől, valamint az elemzés hatékonyságától függ, az egyik elem hatékonysága, a másik nélkül értékét veszi.



5. ábra Egy tipikus honeypot felépítése

Az egyes alrendszerek részletesen bemutatásra kerülnek cikkem második felében.

[10] Az alkalmazás részét képezi a Backtrack live CD alapú linux disztribúciónak
[11] A SET program Website Attack Vectors \ Site Cloner funkciójának felhasználásával

HONEYPOT FELHASZNÁLÁSI LEHETŐSÉGEK

Fontos kiemelni, hogy a honeypot rendszerek támogató védelmi szolgáltatásokat biztosítanak. Indirekt módon támogatják a biztonsági kontrollokat, ami annyit jelent, hogy közvetlen céljuk nem a támadás megakadályozása, hanem annak megértése, ismeretek gyűjtése a hatékony védelem kidolgozása érdekében. Az alábbiakban felsorolom azokat a felhasználási módokat, melyek elősegíthetik a hálózat védelmének fokozását.

Riasztás

Korai riasztási rendszerként (un.: Early Warning System) használva, a honeypot értesíti az üzemeltető állományt a biztonsági incidens bekövetkeztéről. A belső hálózaton terjedő férgek, felderítést végző hacker eszközök (*hacker tools*) forgalmat generálnak a riasztási rendszer IP tartománya (csalijainak) irányába, elárulva ezzel tevékenységüket.

Forgalom klasszifikációja

Internetszolgáltatók (ISP), incidenskezelő szervezetek (CERT) és globális hálózattal rendelkező szervezetek (pl.:kormányzati vagy gazdasági szektor) a honeypotok segítségével képessé válnak (a felhasználói jogok, adatvédelmi törvények megsértése nélkül) a kártékony forgalom szeparált megfigyelésére, valamint a fertőzött, támadó jellegű végpontok forgalomból történő kizárására.

Nagy intenzitású járványok (pl.:Slammer, CodeRed, Nimda, Blaster, Conficker stb.) esetén akár a végpontok karanténba helyezésével, a kártékony kód vezérlőcsatornájaként üzemelő hálózati végpontok lekapcsolásával, vagy szimulálásával (pl.:DNS rekordokba az adott kártékony domain IP-je helyett egy, a fertőtlenítés lépéseit leíró weblap címe kerül) is elősegíthetik a védekezést. Ennek a módszernek az alkalmazására már láthattunk példát az utóbbi években, például a coreflood [8] és a bredolab [9] botnetek esetén.

Információszerzés, tudásbővítés

Segítségével az üzemeltető állomány megismeri a támadó eszközeit, módszereit és céljait, elősegítve ezzel a naprakész védelem fenntartását.

A globális méretű csali és szenzorhálózatok lehetőséget biztosítanak az egyedi támadási módszerek elemzése mellett, a támadási trendek statisztikai analízisére. A világméretű hálózat segítségével az automatizált (hálózati férgek, alacsony tudásszintű, csak a mások által elkészített támadóeszközöket használó „script kiddie”-k) és a célzott támadások statisztikai módszerekkel megkülönböztethetőek. Hiszen ha több szenzortól gyűjtött naplóban is jelentkezik, ua. a forráscím által generált forgalom, ugyanolyan paramétereket, metaadatokat tartalmazó hálózati csomagokat, akkor azok azonos támadó platformról érkeznek[12].

Naplózás, mintagenerálás

A támadások és a kártékony kódok jellegre leginkább magához az Internethez hasonlíthatóak:

- dinamikusan változnak, adaptálódnak és frissülnek a technológiai fejlődéssel párhuzamban;
- nehezen kategorizálhatóak, nincsen egy mindenre kiterjedő katalógus, egységes rendező elv.

Mivel céljuk az egyediség, az újítás, nehezen írhatóak le, definiálhatóak a vírusadatbázisok számára. A honeypot működése során rögzíti a támadás forgatókönyvét,

[12] Legyen az botnet álal vezérelt, kompromittálódott végpont, un. „zombie” gép, vagy „script kiddie” által használt, "hangos" támadóeszköz.

valamint más biztonsági funkció támogatása érdekében mintákat készít a használt támadási technikáról. A behatolás megelőző rendszerek mintáinak[13], vírusirtó szignatúráknak (Antivirus signature) előállításával a későbbi detektálást gyorsítja fel (hasonlóan a biológia immunrendszer ellenanyag termeléséhez[10]).

Preventív védelem

Az úgynevezett tarpit, vagy "sticky honeypot" a támadó felderítő tevékenységét lassítja, hamis célok és lassú válaszidő segítségével.

Ennek a felhasználási módnak az alkalmazása hasonlít leginkább a valós csapdák funkciójára: hiszen célja, hogy minél tovább feltartoztassa-foglalkoztassa a behatolót.

Digitális nyomforrás[11]

Az elkövető ellen kezdeményezett jogi lépések egyik alappillére lehet a csali alrendszeren létrejött, a szenzor alrendszerrel hitelesen, és pontosan rögzített bizonyíték.

A Toulouse Egyetem [12] egyik kutatása kifejezetten a magas interakciójú honeypotok elemzésére, a támadó entitások klasszifikációjára fókuszál. A saját üzemeltetésű honeypotjaik naplóiból készített statisztikák, és a kiemelt minta-esetek segítségével demonstrálják az automatizált, és az emberi támadók által hagyott nyomok közti különbséget (gépelési hibák, bufferelt vagy karakterenként gépelt parancsok, gépelési sebesség, logikai hibák, a rendelkezésre álló információktól független, programozott feladat-végrehajtás, a kompromittált gép használatának céljai, stb.).

Audit eszköz

Kutatómunkám során számos esetben találkoztam, a honeypotok tulajdonságait részben vagy egészben felhasználó rendszerekkel (pl.: malware elemző környezetek[14]), valamint a veszprémi CheckVir tesztlabor[15] rendszerével (a kutatás eredményeit részletesen publikálta Leitold Ferenc [13]). Ennek a labornak a célja, hogy a különböző gyártók, fejlesztők víruskereső alkalmazásait a teljesítmény és hatékonysági paramétereik alapján, objektív módszerekkel értékelje. A tesztlabor kialakítása, működési elve egy magas interakciójú kliens honeypotokból álló hálózatra emlékeztet.

Természetesen számtalan más, védelmi célú eszköz tesztelésére biztosít lehetőséget egy honeypot rendszer. A csali rendszereket használhatjuk akár az automatizált sérülékenység-kereső eszközök (un.: vulnerability scanner) működésének ellenőrzésére, vagy a különböző tűzfal, behatolás-detektáló eszközök összehasonlítására, terhelési vizsgálatára (elkerülve ezzel az üzemelő rendszer működésének veszélyeztetését).

Nem legális alkalmazás

A védelmi célú, „jó-szándékú” alkalmazások mellett említést kell tenni az elkövetők által alkalmazható honeypotokra is, melyek az ellentámadások (melyet elsősorban a vetélytárs bűnszervezetek indítanak) detektálására, valamint a konkurencia technológiáinak kifürkészésére irányul. Hatékonyan alkalmazhatják az új támadási vektorok gyűjtésére, a botnetek parancscsatornájának kifürkészésre és a kontroll átvételére. Továbbá a publikusan elérhető eszközöket tanulmányozhatják, saját védelmük fokozására a honeypotok detektálásra ellenintézkedések dolgozhatnak ki (LÁSD pl.: virtualizáció detektálása), az implementációkban sérülékenységeket kereshetnek (a honeypotok kompromittálása érdekében).

---

[13] IDS signature

[14] Ilyenre példa a *High Security Lab* által üzemeltett *Network Telescope* elnevezésű kártékony kód gyűjtő rendszere, mely megtekinthető az alábbi URL-n: http://lhs.loria.fr/index.php?option=com_content&view=article&id=94&Itemid=84

[15] A kutatólabor technikai felépítése az alábbi linken érhető el: http://www.checkvir.hu/methodology

ÖSSZEFOGLALÁS

A csali és szenzor rendszerek a biztonság kialakításának és fenntartásának egy új megközelítését sugallják:

- A védelem hatékonysága nemcsak az egyes funkciók (jogosultság kezelés, határvédelem stb.) meglétététől, hanem azok naprakészségétől, felügyeletétől és összhangjától is függ[16].
- A fenyegetettség mértéke folyamatosan változó érték, a bekövetkezés valószínűségét nem lehetséges a védelmi kontrollokkal 0-ra csökkenteni (maradvány kockázatot feltételezünk).
- Nem elégséges az ismert támadási módok szűrése, folyamatosan készülni kell az ismeretlen fenyegetések kezelésére.
- A preventív kontrollok hatékonysága azok naprakészségétől függ.

Ez az új szemlélet a támadásokat megakadályozása mellett azok megértését (sérülékenység oka, támadó módszere, és az indok) is szükségesnek tartja.

Jelen írásom célja a honeypot rendszerek általános jellemzőinek, felépítésének bemutatása, annak érdekében, hogy az informatikai biztonsággal foglakozó kutatók (kártékony kódelemzők, hálózatbiztonsági szakemberek, tanácsadók stb.) számára megfelelő tudásbázist képezzen. Segítségével a céljaiknak, elvárásaiknak leginkább megfelelő rendszer tervezése, implementálása valósulhat meg.

A honeypot rendszerek vitathatatlan előnye, hogy képesek az incidensek teljes „életciklusa" alatt támogatni a védekezést. A bekövetkezés előtt képes nyomokat rögzíteni (detektív jelleg) a támadás korai fázisáról[17]. A preventív funkciókat indirekt módon, a támadó szándékának, „érdeklődési területének" jelzésével támogatja. A támadási kísérletek azonosítása (detektív és reaktív funkciók), hozzájárul az üzemeltetési rendszabályok és praktikák naprakészen tartásához, a sérülékenységi minták generálásához (szűrés), a konfigurációs és implementációs hibák kijavításához (sérülékenység megszüntetése).

A honeypotok felhasználási lehetőségeivel és működési elvével általánosságban foglalkozó kutatók, valamint az egyes eszközök leírásainak összevetése során észrevettem, hogy a működési elvek és alkalmazott technológiák szempontjából a valós implementációk nehezen kategorizálhatóak (általában több típus definíciójának is megfelelnek). Így összehasonlításuk, hatékonyságuk értékelése nehézkes. Ez a tény ösztönzött, a honeypotok működési elveinek és felhasználási lehetőségeinek összegyűjtésére, valamint további módszerek és lehetőségek kutatására.

Cikkem második felében, az első témakörhöz szorosan kapcsolódó területtel foglalkozom: a honeypot rendszerek felépítésével, alkotórészeivel (Csali alrendszer, szenzor alrendszer, elemző alrendszer). A kutatásom során szerzett tapasztalatok, bevált gyakorlatok említése mellett kitérek a témát érintő aktuális kutatásokra is.

Felhasznált irodalom

[1] Krasznay Csaba*: Kockázatkezelés – előadásanyag (online)*
Forrás: www.krasznay.hu/presentation/elte_02.ppt
letöltve: 2011.10.03

[16] Erre jó példa, hogy nem elégséges a biztonsági eseményeket rögzíteni (naplózni), hanem a különböző források (tűzfal-, authentikációs szerver-, szolgáltatás naplók) korrelációja és azok feldolgozása is szükséges (üzemeltető állomány értesítése, vagy automatikus reakció).

[17] Pl.: a támadó, vagy a kártékony kód a hálózat aktív IP címmel rendelkező végpontjait keresi, nyitott portokat és sérülékeny szolgáltatásokat azonosít

[2] *Behatolásdetektálás, IDS rendszerek – előadásanyag (online)*
Forrás: http://www.sze.hu/~heckenas/okt/ids.pdf letöltve: 2011.10.03

[3] *Red Hat Enterprise Linux 4.5.0 - Security Guide* - 9.1.1 fejezet (online)
Forrás: http://www.centos.org/docs/4/4.5/Security_Guide/s2-ids-types.html letöltve: 2011.10.03

[4] *Intrusion Detection System Overview Summary* oktatóanyag (online)
Forrás: http://ciscoarticles.com/CCSP-Cisco-Certified-Security-Professional/Intrusion-Detection-System-Overview-Summary.html letöltve: 2011.10.03

[5] Kassai Károly: *A Magyar Honvédség információvédelmének - mint a biztonság részének- feladatrendszere: doktori (PhD) értekezés* (2008), pp. 75-76.
Forrás: http://193.224.76.4/download/konyvtar/digitgy/phd/2008/kassai_karoly.pdf letöltve: 2011.10.03

[6] Lance Spitzner: *Build A Honeypot* (online)
Forrás: http://www.spitzner.net/honeypot.html letöltve: 2011.10.03

[7] Lorie W. Carter: *Setting Up a Honeypot Using a Bait and Switch Router*
Forrás:http://www.sans.org/reading_room/whitepapers/casestudies/setting-honeypot-bait-switch-router_1465 letöltve: 2011.10.03

[8] *US Government Takes Command of Coreflood* (online cikk)
Forrás:http://articles.yuikee.com.hk/newsletter/2011/04/a.html letöltve: 2011.10.03

[9] Landelijk Parket: *Dutch National Crime Squad announces takedown of dangerous botnet*
Forrás:http://www.om.nl/algemene_onderdelen/uitgebreid_zoeken/@154338/dutch_national_crime/ letöltve: 2011.10.03

[10]Jeffrey O. Kephart: *A Biologically Inspired Immune System for Computers*
Forrás:http://www.research.ibm.com/antivirus/SciPapers/Kephart/ALIFE4/alife4.distrib.html letöltve: 2011.10.03

[11] Illési Zsolt: *KRIMINÁLTECHNIKA SZEREPE AZ INFORMATIKAI VÉDELEM TERÜLETÉN,* Hadmérnök IV. Évfolyam 1. szám - 2009. március (online), p. 177, ISSN 1788-1919 Forrás: http://hadmernok.hu/2009_1_illesi.pdf letöltve: 2011.10.03

[12] E. Alata, V. Nicomette, M. Kaâniche, M. Dacier, M. Herrb: *Lessons learned from the deployment of a high-interaction honeypot* (online)
Forrás: http://arxiv.org/ftp/arxiv/papers/0704/0704.0858.pdf letöltve: 2011.10.03

[13] Leitold Ferenc: *VÍRUSVÉDELEM KIVÁLASZTÁSA*, Hadmérnök IV. Évfolyam, 4. szám, 2009. március (online), ISSN 1788-1919
Forrás: http://hadmernok.hu/2009_4_leitold.php letöltve: 2011.10.03

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Tibenszkyné Fórika Krisztina
tibinszkyne.forika.frisztina@uni-nke.hu

A KATONAI FELHŐ BÉKÉS VILLÁMAI: A HONVÉDELMI CÉLÚ SZÁMÍTÁSI FELHŐ LÉTREHOZÁSÁNAK LEHETŐSÉGEI ÉS VESZÉLYEI

Absztrakt

A cloud computing napjaink ígéretes IT technológiája, amely gyakran foglalkoztatja a szakembereket, akik az újdonságok alkalmazásának lehetőségeit kutatják. A kormányzati szféra és a honvédelem is olyan terület, ahol érdemes a "felhőprogramozás" alkalmazhatóságának lehetőségeit megvizsgálni. A szerző a cikk első részében bemutatja a felhő számítási modell kialakulásának folyamatát, rétegeit és szolgáltatásait, illetve főbb típusait, majd elemzi a különböző cloud computing alkalmazások előfordulási arányait a tudományos életben területenként és földrészenként. A szerző felvonultat néhány amerikai hadseregben alkalmazott felhő modellt, majd egy olyan - magyar hadseregben alkalmazható- alkalmazás tesztelési eredményeit, amely a pályaalkalmassági vizsgálat értékelését segítheti a felhő segítségével, különböző platformokon. A szerző felveti a felhő alkalmazásának jogi és biztonsági kérdéseit a védelmi szférában.

In our days cloud computing is a promising IT technology, which often occupy those experts exploring applications of new technologies. Just like in our everyday life, it is rewarding to examine the possibilities of cloud programming both in the Administration and in the Defense Sector, as well. The author analyses the development phases of cloud computing models, its layers and services, also its relevant types. Later, the author analyses the occurrence ratio of the different cloud computing applications both geographically and thematically. The author lines up some cloud models used in the U.S. Army and then an application that is in use at the Hungarian Armed Forces for analyzing of the results of the physical competency testing for soldiers. The author also raises the important issue of the legal and security aspects for using cloud computing technology within the Defense Sector.

Kulcsszavak: *számítási felhő, felhőalkalmazások, pályaalkalmassági vizsgálat, védelmi szféra ~ cloud computing, Defense Sector, cloud applications*

BEVEZETÉS

A cloud computing napjaink ígéretes IT technológiája, amely gyakran foglalkoztatja a szakembereket, akik a gazdaságosság, egységesség és biztonság szempontjából az újdonságok alkalmazásának lehetőségeit kutatják. A kormányzati szféra és a honvédelem is olyan terület, ahol érdemes a felhő programozás alkalmazhatóságának lehetőségeit megvizsgálni. A közelmúltban a magyarországi önkormányzati hivataloknál bevezetett „kormányablak" szolgáltatás, e-ügyintézés a kormányzati adatok egyszerűbb és központosított elérését teszi lehetővé, ami a felhőalkalmazásoknak is sajátossága. Jelen cikkben megvizsgálom a felhő számítás alkalmazhatóságának előnyeit, feltételeit és veszélyeit a védelmi szférában. A cikk első részében a felhő felépítésével, típusaival és platformjaival foglalkozom, majd a következő részben azt vizsgálom, hogy a számítási felhő alkalmazása jelenleg mennyire elterjedt a világban, és milyen felhőtípusok találhatóak jelenleg a védelmi szférában, majd bemutatom egy védelmi célú felhő modell lehetséges felépítését, előnyeit és kockázatait.

ÁLTALÁBAN A SZÁMÍTÁSI FELHŐ MODELLRŐL

Ha a cloud computing kifejezést halljuk, vagy olvassuk, számos kérdés felmerülhet bennünk, amelyek megválaszolása azt igényli, hogy mielőtt a technológiát el- vagy megítélnénk, megnézzük mikor is alakult ki, van e gazdasági jelentősége, milyen szolgáltatásokat biztosít és kik vehetik igénybe. A következőkben arra teszek kísérletet, hogy bemutassam, hogyan is alakult ki a „cloud", és milyen szolgáltatásokat biztosíthat a felhasználóknak.

A felhő története

A számítási felhő fogalma az utóbbi 5 évben terjedt el, ugyanakkor a fejlődése az elmúlt évtizedben kezdődött. A 90-es években a clusterek használata terjedt el. A cluster egyfajta típusa a párhuzamos elosztott rendszereknek. Összekapcsolt, önálló számítógépek gyűjteménye, amelyek integrált számítógép erőforrásként dolgoznak együtt. A cluster-ek olyan adatközpontokkal álltak kapcsolatban, amelyek tudományos, üzleti, vállalati problémák megoldását hivatottak segíteni. 2000-től a grid computing vált népszerűvé. A számítási grid egy hardver és szoftver infrastruktúra, amely megbízható, konzisztens, mindent átható, és olcsó hozzáférést biztosító számítási képességek kibontakozását tette lehetővé azáltal, hogy földrajzilag elosztott erőforrásokat kapcsolt össze, mint a szuperszámítógépek, clusterek és adattárak. Míg a clusterek és gridek viszonylag szűk felhasználói réteg számára kínáltak gyors computing szolgáltatásokat, 2008-tól a cloud computing már az elosztott és párhuzamos rendszerek használatát virtuális gépek szolgáltatás szintű felhasználását tette lehetővé. Ha megnézzük a Google keresőjének segítségével a cloud-, grid- és cluster computing népszerűségét az elmúlt 10 évben, akkor megfigyelhető a felhő népszerűségének meredek növekedése az utóbbi 3 évben. (1. ábra)

1. ábra. A számítási felhő népszerűségének alakulása az utóbbi években
Forrás: Google Apps 2011.03.10.

A cloud computing rétegei és szolgáltatásai

Az internetes funkciók meghatározása során többfajta hálózati protokollon vezet az út, az ISO-OSI modell rétegei jól megfigyelhetők. Ha két számítógép között cloud computing kapcsolat épül fel, a rétegek együttműködését kihasználva az alábbi szolgáltatások megosztását végezhetjük el. A cloud computing modell rétegei egymásra épülnek akár egy piramis építő kövei.

Fizikai réteg mint szolgáltatás (Iaas – Infrastructure as a Service)

A fizikai réteg a cloud computing szolgáltatások megvalósítását biztosító hardware infrastruktúra. Ez a felépítés legalsó és legalapvetőbb rétege. Ezen múlik az igénybe vehető magasabb rendű szolgáltatások minősége. Ide tartoznak a szerverek, clusterek, gridek, adatbázisok, összekapcsoló eszközök, amelyekre a virtuális infrastruktúra épül. Az infrastruktúra nagyszabású cloud alkalmazásoknál többnyire száz vagy akár ezer gép támogatásával valósul meg. Ide tartoznak a különböző hosting szolgáltatások, Internet szolgáltatás és a helymegosztás. A fizikai réteg erőforrásait virtuális gépek segítségével vehetik igénybe a felhasználók.

Virtuális erőforrások mint szolgáltatás (Virtual Infrastructure as a Service)

A virtuális erőforrások olyan gépek, amelyeken a felhasználó tetszőleges alkalmazásokat futtathat és vehet igénybe. A virtuális infrastruktúra, mint szolgáltatás virtuális számítógépet biztosít szolgáltatásként. A felhőben történő infrastrukturális szolgáltatások, komplett számítógépes infrastruktúrákat tesznek elérhetővé többnyire platform virtualizáció segítségével. A virtuális gép sablonok között lehet logikai meghajtó, VLAN hálózat, rendszer management és a felhasználó kiválaszthatja a számára legalkalmasabbat igény szerinti operációs rendszerrel, adatbázis kezelővel vagy web szerverrel. Az ügyfelek ahelyett, hogy megvennék a szükséges erőforrásokat (szerverek, hálózati eszközök, szoftverek, adatközponti elhelyezés, stb.) azokat szolgáltatásként megvásárolva teljesen kiszervezett informatikai szolgáltatást vesznek igénybe. A szállítási szerződésekben jellemzően az „elfogyasztott” számítási teljesítmény alapú számlázás jelenik meg, mely a közüzemi szolgáltatásokhoz hasonlóvá teszi a XX. században oly különleges informatikai szerepeket. Az ilyen formában bérelhető virtualizált szerverek piacán az ügyfelek válogathatnak a szolgáltatók közül. A virtuális gépeken nyílt forráskódú vagy fizetős szoftverek vannak telepítve, amelyek felett a felhasználó teljes körű felügyelettel rendelkezik és igény szerint testre szabhatja. A felhasználók szétkülönítését a virtualizáció biztosítja.

A felhasználói réteg, mint szolgáltatás (PaaS - Platform as a Service)

A cloud computing ötvözi a grid és cluster computing tulajdonságait, ami elősegíti a virtualizációt, amin a különböző webes szolgáltatások megvalósíthatók. A felhő platform

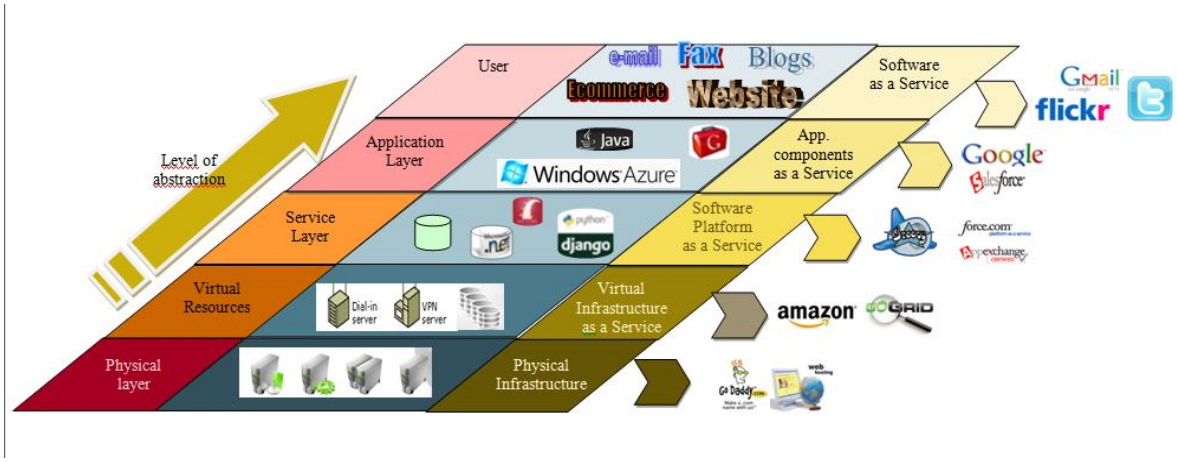
szolgáltatás lényege, hogy az ügyfél szolgáltatásként veszi igénybe a működő számítástechnikai platformokat, alap infrastruktúrákat pl. web szerver. A szolgáltatás által biztosított infrastruktúra alapul szolgálhat az alkalmazások elhelyezésére. Az így létrejövő megoldás lényege, hogy a szolgáltatásként megvásárolt felhő infrastruktúra fenntartása és üzemeltetése megvásárolható, függetlenül annak komplexitásától. További költségcsökkentő tényezőként hat, hogy az alkalmazások fejlesztésére sem kell erőforrásokat áldozni. A felhők szolgáltatást biztosítanak a felhasználóknak anélkül, hogy számítana, milyen infrastruktúrával veszik azt igénybe. A platform mint szolgáltatás számítási platformot és vermet biztosít, mint szolgáltatást. A szolgáltatás rugalmas, könnyen testre szabható és kiterjeszthető platformokat biztosít, amelyek segítségével alacsony költségek mellett lehet alkalmazás tervezést, fejlesztést, tesztelést végezni. Lehetővé teszi adatbázisok csatolását, biztonsági kérdések, skálázhatósági kérdések megoldását. A felhasználó táv vezérelheti, felügyelheti és dinamikusan változtathatja, ami fontos nem csak a kontrollálásának, hanem azonosításának és megszűntetésének érdekében is.

Az alkalmazási réteg, mint szolgáltatás (Application Component as a Service)

Az alkalmazási réteg, mint szolgáltatás**,** biztosítja a különleges alkalmazás specifikus interfészeket (API) az alkalmazások beépítéséhez. Olyan web alapú software szolgáltatás, amely segítségével újabb szolgáltatások építhetők ki. Sok elismert platform van, mint pl. a Google. App. Engine vagy a SalesForce Force.com alkalmazás. A legtöbb Java alapú, de .Net keretrendszert használó vagy Azure alkalmazást is találunk a Paas szolgáltatások között.

A felhasználó réteg, mint szolgáltatás (SaaS - Software as a Service)

A felhőben történő alkalmazás szolgáltatást az ügyfelek az Internet segítségével vehetik igénybe, így az ügyfél számítógépén (kliens eszközén) nem szükséges kliens programot telepíteni. A szolgáltató biztosítja a szoftvert, amit a felhasználó online használ. Ez a tulajdonság üzemeltetési szempontból nagyon kedvező, mert jelentősen egyszerűsíti a karbantartást és a támogatást. Az alkalmazások lehetnek kereskedelmi forgalomban megjelenő (esetleg ingyenes, de semmiképp sem egyedi), vagy hálózat alapú hozzáférést és kezelést biztosító szoftverek. Az alkalmazásokhoz hozzáférés biztosítható az interneten keresztül központi helyszínen kezelve, a több kisebb telephellyel szemben. Az alkalmazásokat jellemzően többen (akár különböző ügyfélkörök) használhatják, és a használatban az „egy a többhöz" típus jellemző (Google Dokumentumok) az „egy az egyhez" típussal szemben (pl.: célszoftverek). A szolgáltatás központosítása, egyszerűsíti a frissítési, karbantartási feladatokat és szükségtelenné teszi a klienseken történő alkalmazás-frissítési folyamatokat. Annak a lehetősége, hogy a felhasználók különféle legújabb alkalmazásokat használjanak, soha nem volt nagyobb.



2. ábra. A felhő típusok és az ISO rétegek kapcsolata
Forrás: saját készítés

A számítási felhők típusai

Nyilvános felhő

A felhőket klasszikus megjelenési formában „nyilvánosnak” vagy „külsőnek” is nevezett felhőként értelmezhetjük. A nyilvános számítási felhőket létrehozó szolgáltatók elsősorban az Interneten kínálják szolgáltatásaikat, amelyet online akár önkiszolgáló módon lehet igénybe venni. A szolgáltatás paraméterezése már a megrendelés folyamán nagyon pontosan állítható (pl.: hardver igények); majd a szolgáltató segédprogramok segítségével, a ténylegesen használt erőforrások alapján számlázza ki a szolgáltatás költségét, ha van. A belépők köre nem szabályozott, de regisztrációhoz, megrendeléshez kötött.

Közösségi felhő

A közösségi felhő létrehozása több szervezet általi együttműködésből is származhat. Amennyiben azonos elvárásokkal, követelményekkel közösen használt infrastruktúrákat hoznak létre, megvalósulhatnak a számítási felhők adott jellemzői. A költségek ebben az esetben már jóval kevesebb felhasználó között oszlanak el, mint a nyilvános felhők esetén, tehát a megoldás drágább azoknál, de a szükséges adatvédelmi, biztonsági, akár politikai megfelelés ilyen formában biztosítható (pl.: a Google „Gov. Cloud” megoldása, vagy a Microsoft Business Productivity Online Suite megoldása).

Hibrid felhő – kombinált felhő

A hibrid felhő kifejezés különféle felhők (állami-, magán-, külső- vagy belső-) összekapcsolása esetén jelenik meg. Amennyiben az egyes felhőket kiszolgáló infrastruktúra virtualizált, előfordulhat, hogy ugyanazon a host-on többféle felhő modell van jelen. A hibrid felhő jelentéséhez kapcsolható továbbá az is, hogy egy felhőben a virtualizációs technológia mellett hagyományos fizikai hardveren alapuló technológia is részt vehet a szolgáltatásban. A jövőben várható a kombinált felhő szolgáltatások elterjedése, jellemzővé válhat az informatikai infrastruktúrák ilyen jelegű felépítése, átépítése. Ez a modell teremtheti majd meg az átmenetet a nyilvános felhők és a közösségi (állami) felhők között, így áthidalhatóvá - de nem elhagyhatóvá - válik az utóbbinál felmerülő biztonsági megfelelés kérdésköre. A webes alkalmazások felhőben történő elhelyezése (Hybrid Web Hosting) mellett erre a célra dedikált fizikai hardver elemeken (szervereken) futó példányok használatával internetes cluster-ek valósíthatók meg. Egyes példányok a fizikai infrastruktúrán, mások a felhő szerveren futnak. Hibrid felhőként értelmezhetők továbbá a közösségi és privát felhőkből álló adattároló felhők. Ezeket legtöbbször archiválásra és biztonsági mentésre használják, így lehetővé válik helyi adatok replikálása.

Privát felhő

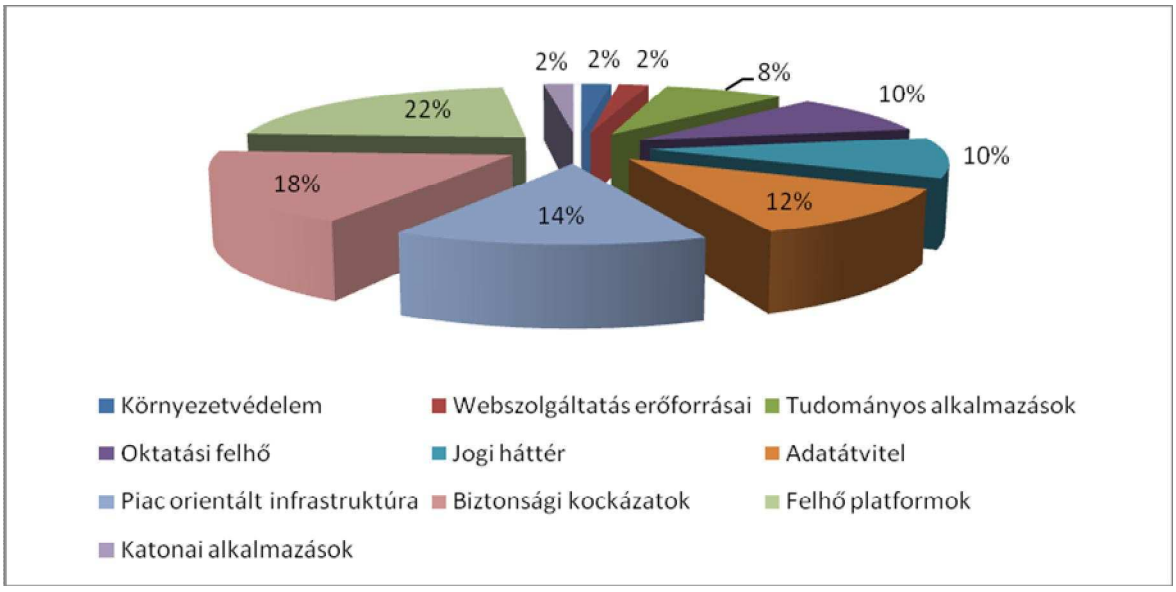
Az üzemeltetési költségek és a kockázatok egyensúlyát a kisebb informatikai eszközparkkal rendelkező szektorokban a legnehezebb megteremteni. A rendelkezésre álló erőforrásokat optimalizálni kell, így előtérbe kerülnek a virtualizációs technológiák. Az üzemeltetést saját eszközparkkal megoldva, az erőforrás hiányra az alkalmazások, szerverek virtualizációja jelenheti a megoldást. Ennek automatizálásával jönnek létre azok a privát felhők, amelyek meg tudnak felelni a rendelkezésre állási-, helyreállíthatósági-, skálázhatósági követelményeknek. A költségek tervezése és felmerülése így követhetővé válhat. A privát felhők bár a felhasználók általi beruházásból jönnek létre, de azokat fel kell építeni, üzemeltetni kell. A beruházási kényszer és az adatvédelmi előírásoknak, elvárásoknak való megfelelés összefüggései itt jelennek meg a legmarkánsabban. A számítási felhő technológia használatának további lehetőségét a gazdasági kényszerhelyzetek „teremthetik meg”.

MIRE HASZNÁLJÁK A FELHŐT KÖRNYZETÜNKBEN?

A különböző felhőszolgáltatások és típusok ismeretében felmerülhet bennünk a kérdés, hogy milyen alkalmazások valósulnak meg a modellek segítségével a környező országokban. A következőkben azt vizsgáljuk meg, hogy a tudományos életben mennyire foglalkoztatja a tudósokat ez az IT szolgáltatás. A tudományos élet aktivitása szerintem meglehetősen jól tükrözi a felhasználói aktivitást is az adott térségben.

A felhő szolgáltatás rendszerezése országonként, típusonként

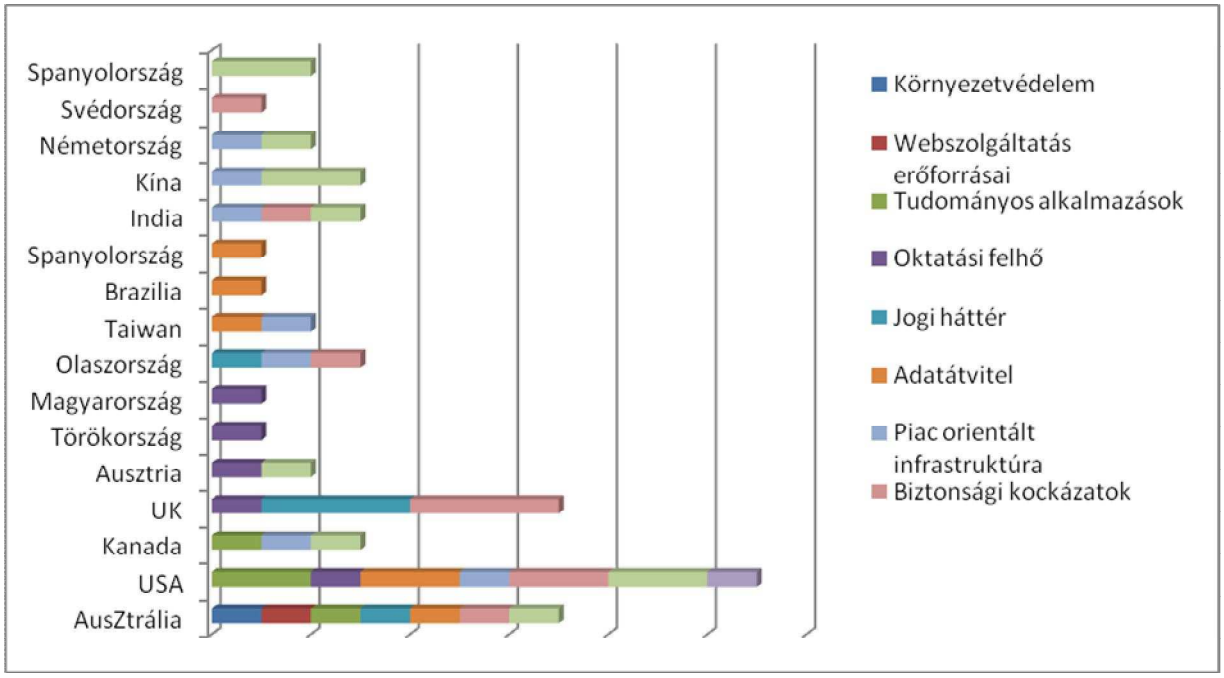
A felhő alkalmazások országonként térségenként eltéréseket mutatnak. Megvizsgáltam a tudományos élet publikációit a témában, és azt találtam, hogy a kutatások nagy részét a különféle platform megnyilvánulások alkotják, ugyanakkor a felhő modell alkalmazásának biztonsági kérdései foglalkoztatják következő legnagyobb mértékben a tudományos élet szereplőit. Ez részben azt bizonyítja, hogy az adatok biztonságos kezelésének, tárolásának, elérésének kérdései nem egészen szabályozottak és kidolgozásuknak, alkalmazásuknak miként tjében a kutatók különböző módszereket ajánlanak. (3.ábra) A művek 14 %-át a piac orientált felhő architektúrák bemutatásai alkotják, ami a felhőgyár anyagi vetületének hatalmas jelentőségét mutatja. Az adatok közvetítésével, továbbításával és elérésének eszközeivel foglalkozó művek 12%-ban fordultak elő, ami nagy számú gyakorlati szakember kérdései megoldásait mutatja a témában. A jogi kérdések feszegetése, az oktatás és a kutatás körülbelül egyenlő arányban foglalkoztatja a tudományos társadalmat, míg elenyésző a felhő szolgáltatások elveivel és környezeti hatásainak elemzésével foglalkozó cikkek elenyésző számban fordultak elő.



3. ábra. Felhő szolgáltatások típusainak eloszlása
Forrás: saját készítés

Ha megnézzük a tudományos élet mozgalmasságának területi elosztását, tehát, hogy melyik kontinensen foglalkoztak a legtöbbet a Felhővel, akkor természetesen az Amerikai Egyesült Államok vezeti a rangsort, ahol a kutatások minden szegmense előfordul. Ugyanakkor Angliában a jogi, biztonsági kérdések feszegetése a legelterjedtebb a felhők oktatásra történő felhasználása mellett. Ausztráliában szintén mindenfajta kutatás előfordul. Kína, India, Olaszország, Kanada jelentős kutatásokat végez a témában, Magyarország, Törökország, Spanyolország, Svédország szintén folytat felhő kutatásokat. Ugyanakkor, míg Magyarországon többnyire az oktatási célú alkalmazások használata a legelterjedtebb,

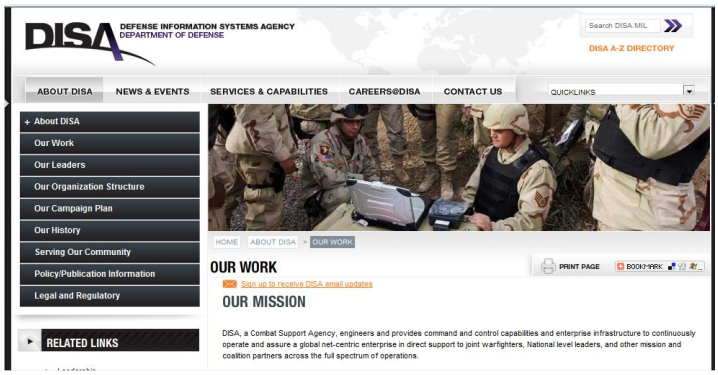
Spanyolország és Brazília az adatok közvetítésének problematikájával foglalkozik. Mindössze egy olyan országot találtam, ahol katonai alkalmazások Felhőben történő megvalósításának kutatásairól tudományos cikket publikáltak, és ez Amerikai Egyesült Államok. (4. ábra)



4. ábra. Felhőszolgáltatások típusainak eloszlása földrészenként

Katonai felhő alkalmazások

Az amerikai hadsereg bekapcsolódását a cloud szolgáltatásokba a DISA (Defense Information Systems Agency) kontrolálja. A 21. században a sikeres harci és békeműveletek követelményei gyorsan változnak. Válaszul az aszimmetrikus fenyegetések, és a kiszámíthatatlan ellenfél felbukkanásának veszélye ellen, az Amerikai Védelmi Minisztérium (Department of Defense, DoD) történelmi átalakuláson megy keresztül. Az amerikai minisztérium információs rendszerekkel foglalkozó ügynöksége, a DISA (Defense Information Sytems Agency) olyan katonai felhő alkalmazási modellt hozott létre, amelyben számos szervezet vesz részt, és felöleli a missziós-, politikai-, biztonsági-, minőségbiztosítási területeket is. A parancsnoki és irányítási (Command and Control Systems, C2) rendszerek lehetővé teszik az információs fölény megszerzését a csatatéren. Biztosítják a parancsnok számára azokat az információkat, amelyeknek segítségével hatékony döntéseket hozhatnak. (5. ábra).



5. ábra. DISA felhő
Forrás: www.disa.mil

Az egyik ilyen szolgáltatás, amelyet a DISA használ a Védelmi Online Kapcsolat (Defense Connect Online, DCO), amely biztosítja a katonák és parancsnokaik számára, hogy együttműködhessenek a világ bármely részéről.(6. ábra)

6. ábra. DCO Kapcsolat kiépítése
Forrás: www.adobe.com/government/dco

Az amerikai hadsereg kiépítette a gyors elérés lehetőségét a különböző katonai alkalmazásokhoz RACE néven (Rapid Access Computing Environment, RACE), amelyen belül a Forge.mil alatt olyan alkalmazások érhetőek el, amelyeket a hadseregen belül általánosan használnak. A RACE támogatja az ilyen célú alkalmazások fejlesztését is, akár fejlesztési versenyek hirdetésével is. A modell lehetővé teszi a közös fejlesztést, és a nyílt forráskódú illetve a DoD közösségben használt szoftverek elérését is. (7.ábra) Ilyenek például azok a minden katonai szervezetnél használt alkalmazások, mint pl. a Munka ideje (Work Time), a Toborzás (Recruiting), és a képzési- tanulási rendszer.(Learning Manegement System).

7. ábra. Forge. mil közösségi oldal
Forrás: www.forge.mil

FELHŐ ALKALMAZÁS LEHETŐSÉGE A VÉDELMI SZFÉRÁBAN

A cloud computing korunk egyik egyre dinamikusabban fejlődő információs technológiája amelynek alkalmazási lehetőségeit a védelmi szférában is érdemes megvizsgálni. Az Egyesült Államokban számos példát találunk az alkalmazására és Obama elnök kiemelt feladatként kezeli az alkalmazásának bevezetését. Az egyik fő ok a kormányzati szféra költségeinek csökkentése illetve az adatelérés biztosítása mindenkor, minden eszközön. Magyarországon a NATO tagállamaként számba kell venni, hogy a felhő alkalmazásának melyek lehetnek a fő szolgáltatási típusai, alkalmazások fajtái és milyen veszélyekkel járhat a használata. Ez azt jelenti, hogy ki kell alakítani a felhőszámítással kapcsolatos feladatok rendszerét, melyben mérlegelni kell a lehetséges előnyöket, a költségmegtakarításokat, az elvégzendő feladatokat és a felmerülő veszélyeket. A következőkben néhány gondolatot vázolok az említettekkel kapcsolatban.

A védelmi felhő kialakításainak lehetséges előnyei

A számítási felhő lehetőséget biztosít az adatok automatikus online elérésére, ami megoldhatja a kormányzati és védelmi szférában használt szoftverek sokszínűségének problémáját. A csapatoknál dolgozó informatikus szakemberek gyakran találkoznak azzal a problémával, hogy a felhasználók különböző operációs rendszereken különböző szoftverekkel dolgoznak, ami megnehezítheti az együttműködést, és sokszor az azonos kimeneti formára való konvertálás sok időt vesz igénybe. A számítási felhők igénybevételével biztosítható az egységes alkalmazások használata az azonos típusú szervezeteknél, amely elmozdulást jelentene a kézi vezérléstől az ismételhetőség felé. A számítási felhő biztosítja a különböző komponensek, folyamatok újra felhasználását. A számítási felhő költségtakarékos volta engedi a felhasználókat az új szoftverek használatára összpontosítani és mentesíthet a tőkekiadásoktól. Nagy adatbázisok kezelésének és elérésének lehetősége különböző tudományos vagy katonai számítások elvégzése céljából. Jobb hozzáférés az elosztott adatbázisokhoz. Automatikus mentés és költséghatékony archiválási lehetőség. Mivel a felhő szolgáltatások eléréséhez internet kapcsolat szükséges, amely számos eszközzel megvalósítható (PC, laptop, PDA, mobiltelefon) a bejelentkezett felhasználó számára az elérhetőség mindig, bárhol és bármilyen eszközön megvalósítható. Kihasználható az alacsony költségű számítási ciklus és az adattárolás.

Mindezeket figyelembe véve a felhő alkalmazásnak előnyei többek között a következők lehetnek:

- Automatizálás / On-Demand megvalósítás**:**
  - Ismétlődő folyamatok automatizálása és együttműködés;
  - Laborok – előtérben az új szoftverek alkalmazása, nem megvásárlása;
  - Egyszerű használat.
- Egységes platform kialakítása:
  - Elmozdulás az egyéni szoftverektől,
  - Újrahasznosítható változtatható komponensek.
- Költségcsökkenés, átfogó adatorientált kapcsolat:
  - Indexálási képesség, nagy adatbázisok – párhuzamos folyamatok;
  - Jobb adatelérés az elosztott cloud adatbázisokhoz;
  - Automatikus mentés.
- Elérhetőség bármikor, bárhol, bármilyen eszközön
  - Cloud kliens;
  - A kommunikáció kiemelt fontosságú;
  - Platform és geológiai diagnosztika;

- Lehetővé válik a taktikai kapcsolat a hálózat tagjai és résztvevői között.
- Biztonsági lehetőségek javulása
  - Titkosított kliens használható;
  - Lehetséges a rejtjelzett adattárolás;
  - Kötegelt titkosított adatátviteli lehetőség.

Példa egy védelmi célú felhő alkalmazás létrehozására

Napjainkban a katonai fizikai alkalmasság vizsgálata és az erőnlét megléte központi kérdés mind a tisztjelölt hallgatók, mind pedig a hivatásos és szerződéses állomány esetében. *A Honvédelmi Minisztérium 21/2000. (VIII.23.) BM-IM-TNM együttes rendelete* alapján a rendvédelmi szervezetek tanintézeteibe, illetve állományába tartozók pályaalkalmassági vizsgálatát, illetve a MH és HM hivatásos és szerződéses állományának beosztásra való alkalmasságának vizsgálatát rendszeres időközönként el kell végezni.

Jelenleg az állomány fizikai felkészültségének felmérését és értékelését manuálisan, papíron kikeresgélős módszerrel végzik. A teljesítményértékelést nehezíti, hogy számos táblázatban adott előírást és paramétert kell a felmérést végzőknek figyelembe venni a felmérés pillanatában, amely legalább 3 embert igénylő feladat. A Magyar Honvédség elvárásainak megfelelő teljesítmény alapján automatikusan értékelő program és adatbázis kifejlesztése aktuális feladat, amire eddig nem történt kísérlet. A felhő segítségével történő megvalósítás lehetőséget biztosíthat olyan katonai célú alkalmazás készítésére, amelynek elérése bárhol, bármikor, bármilyen internetképes eszköz segítségével megvalósulhat és a katonai pályaalkalmasságra való alkalmasság értékelését minden érdekelt számára lehetővé teszi, legyen az tiszti, tiszthelyettesi vagy tisztjelölti jogállású.

A testnevelő tanárokkal együttműködve, vezetésem alatt, elkészült egy alkalmazás, amely képes lehet a tisztek, tisztjelöltek, civil hallgatók testnevelési és alkalmassági eredményeinek értékelésére és tárolására akár számítógépen, szerveren, androidon vagy mobiltelefonon. A tesztelés alatt álló fejlesztés 3 részből állt össze. Először egy asztali számítógépen használható adattároló és kiértékelő rendszer programja készült el, majd elosztott szolgáltatás létrehozásával megteremtettük a felhőből való elérés tesztelési lehetőségét. A fejlesztés harmadik részében pedig a mobil telefonos megvalósíthatóságát vizsgáltuk. A tesztelési és az alkalmazás-fejlesztési eredmények azt igazolták, hogy megvalósítható olyan, csak a védelmi szférában alkalmazott problémamegoldó szoftver, amelynek felhőből történő elérése lehetséges.

8. ábra. Katonai alkalmasság vizsgáló szoftver elérése mobil eszközön.
Forrás: saját munka

Jogi és biztonsági kérdések

A cloud computing számos jogi és gazdasági kérdést vet fel a kormányzati szervek szempontjából mind a felhőt használók, mind a felhőt alkalmazók szempontjából. Tisztázni kell a hozzáféréssel és a felhasználással kapcsolatos kérdéseket, milyen esetekben van szükség a számítási felhő akadály vagy megszakítás nélküli elérésére. Hogyan biztosítható a felhő megbízhatósága, ha a felhasználók nagy számban egy időben csatlakoznak és nagy memória és háttértár igényű feladatokat futtatnak ugyanabban az időben? *Biztosítani kell* a folyamatos szolgáltatás feltételeit és ki kell dolgozni annak szabályait, mivel a szolgáltatás-kiesés drámai hatással lehet a honvédelmi tevékenységekre és bizalomvesztésen kívül beláthatatlan károkat okozhat. *Ki kell dolgozni* a biztonsági szabályokat, amelyek megakadályozzák a jogosulatlan hozzáférést az adatokhoz, tekintettel a nagy mennyiségű személyes és kormányzati adatokra. *Ki kell dolgozni* a felhőben tárolt bizalmas adatok, a személyazonosításra alkalmas egyedi információk, továbbá bizalmas szervezeti információk kezelésére, módosítására, tárolására és védelmére vonatkozó előírásokat, szabályzókat.

Tisztázni kell az információk, dokumentumok tárolására, archiválására, megőrzésének, titkosításának és megóvásának módjára vonatkozó előírásokat és szabályokat.

A kormányzat *Digitális Megújulási* tervének fókuszában négy fő elem áll, amelyek közül az egyik az Egységes kormányzati IKT-szakirányítás, -tervezés, -felügyelet és – ellenőrzés kialakítása, amelynek érdekében Kormányzati üzemeltető központot hoznak létre. A kormányzati Üzemeltető Központ kialakításának célja, hogy a kiemelt fontosságú rendszerek üzemeltetése kizárólag állami tulajdonban lévő szolgáltató-szervezeteken keresztül, erős szabályozottság mellett történjen. A rendszerek konszolidációja hozzájárul ahhoz, hogy a jogosítványok megfelelő szervezethez rendelésével, a feladatok végrehajtása duplikálás nélkül, kevesebb emberi erőforrással legyen biztosított.[1] Az állam külön jogszabályban határozza meg a kormányzati üzemeltető központ feladatait és kötelezettségeit. Az üzemeltető központ az általa üzemeltetett rendszereken működtetett szolgáltatások vonatkozásában mérhető, egyértelmű, rendszeresen elszámolható és felülvizsgált SLA-alapú szerződést köt az állami fogyasztást összevontan képviselő szervezettel. Az új kormányzati hálózat továbbfejlesztésére a kormány szerint azért van szükség, hogy kiváltsa a számos, egyedileg tervezett, fejlesztett és üzemeltetett, részben elszigetelt állami hálózatokat. Az egységes, közös hálózati infrastruktúra a kormány elképzelése szerint hozzájárulhat az üzemeltetési költségek és a rendszer komplexitásának csökkenéséhez, továbbá új lehetőséget teremt az információk megosztására.

Mindezek alapján úgy tűnik, van szándék egy kormányzati felhő koncepció megteremtésére. Nem tisztázott a koncepció alapján a honvédségi rendszer és alkalmazások integrálásának mértéke és szándéka. Amennyiben a központosítási és konszolidációs szándék a honvédségi hálózatra is vonatkozik, akkor érdemes az előzőekben felvonultatott érveket átgondolni, és ki kell dolgozni a védelmi célú felhő rendszerét, és ki kell képezni a hozzáértő katonákat, közszolgálati személyeket is.

Felhasznált irodalom

[1] http://www.nfm.gov.hu/data/cms2089529/Digitalis_Megujulas_Cselekvesi_Terv.pdf. 54.o., Letöltve 2011.01.16.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Pataki János– Sulányi Péter
janos.pataki@audi.hu - speter@suprex.hu

PERSONENSCHUTZ

Absztrakt/Abstract/Abstrakt

Jelen írás a védett személyek biztosításában közreműködő szervek tevékenységének irányítását elemzi. A cikk bemutatja a védett személyek környezetében kialakított úgynevezett belső biztonsági zóna és a belépésre jogosult személyek operatív ellenőrzésében közreműködő biztonsági szervek munkatársainak feladatait.

This article analyses the control of the security services involved in the activities of protected persons. It describes the security zone around the protected persons and the staff duties in the personal inspections of the entering authorized persons.

Die Sicherheitsbehörde unterstützt und leitet die Tätigkeit von Organisationen, die an der Gewährleistung der Sicherheit geschützter Personen beteiligt sind. Bei der Kontrolle der in der Umgebung der geschützten Personen errichteten sog. inneren Sicherheitszone und der operativen Überprüfung von zutrittbefugten Personen wirken die Mitarbeiter der Sicherheitsbehörde mit.

Kulcsszavak/Keywords/Kernbegriffe: *személybiztosítás, személybiztosítás elemei, különleges védett jármű, Magyarország ~ personal security, elements of personal security, special protected vehicle, Hungary ~ Personenschutz, Elemente des Personenschutzes, Sonderschutzfahrzeug, Ungarn*

"Dann, wenn das Auge geblendet ist und der Mond sich verfinstert
und die Sonne und der Mond miteinander vereinigt werden,
an jenem Tage wird der Mensch sagen:
"Wohin (könnte ich) nun fliehen?"[1]

EINLEITUNG

Der Begriff Personenschutz ist vermehrt auch hierzulande unter dem englischen Begriff "Bodyguard" bekannt. Hierbei handelt es sich um einen Bereich, der durch die verschiedensten Aufgaben geprägt ist. Der Schwerpunkt liegt hierbei auf der Begleitung von Personen. Durch diese sollen unter anderem Belästigungen und Aufdringlichkeiten vermieden und/oder auch zerschlagen werden.

GRUNDSÄTZE DES PERSONENSCHUTZES

Zweck

Personenschutz umfasst die persönliche Sicherheit und Freiheit, die körperliche Unversehrtheit, Gesundheit, die Menschenwürde, die physische und technische Verteidigung einer schutzwürdigen Person (Schutzperson)[2].

Elemente[3]

Die physische Verteidigung

Der Personenschützer führt seine Aufgabe mit physischer Anwesenheit durch und wendet den Anschlag gegen die Schutzperson mit der Anwendung von Gewalt ab.

Die technische Verteidigung

Die Geräte, die die Personenschützer benutzen sind Waffen, Einsatzwesten, Kommunikationsgeräte, Sicherheitsfahrzeuge, Sonderschutz-Fahrzeuge[4] und vieles andere mehr.

Zur technischen Verteidigung bei der Unterkunftssicherung und der Verteidigung des Veranstaltungsortes, werden die Geräte des Objektschutzes (Vermögenschutz: mechanischer Widerstand, Zutrittskontrollsystem, Bewegungsmelder, Videoüberwachungssystem, Brandmeldersystem ...) angewendet.

Gefahranalyse[5]

Die Sicherheitsbehörde unterstützt und leitet die Tätigkeit von Organisationen, die an der Gewährleistung der Sicherheit geschützter Personen beteiligt sind. Bei der Kontrolle der in der Umgebung der geschützten Personen errichteten sog. inneren Sicherheitszone und der operativen Überprüfung von zutrittbefugten Personen wirken die Personenschützer der

[1] Koran (75:7-10)
[2] Reinhard Scholzen: Personenschutz, Stuttgart, Motorbuch Verlag, 2004, Seite 46-50
[3] Reinhard Scholzen: Personenschutz, Stuttgart, Motorbuch Verlag, 2004, Seite 78-102
[4] Reinhard Scholzen: Personenschutz, Stuttgart, Motorbuch Verlag, 2004, Seite 144-161
[5] Reinhard Scholzen: Personenschutz, Stuttgart, Motorbuch Verlag, 2004, Seite 44-45

Sicherheitsbehörde mit. Sie führen umgehend eine entsprechende Datensammlung zur Person und hinsichtlich der Motivation im Falle von Personen durch, die etwaig in die Zone gelangen und sich dort aufhalten — die entstandenen Informationen werden umgehend an die Wachdienste und Sicherheitsorgane weitergeleitet.

Das System für die Organisation des Personenschutzes
Das System des Personenschutzes
Der permanente Personenschutz

Diese schutzwürdigen Personenkreise wurden von der landespezifischen Gesetzgebung bestimmt, und werden ständig – im In- und Ausland – von Beamten der Sicherheitsgruppe begleitet.

Der vorläufige Personenschutz

Personen, die politisch und wirtschaftlich kontroverse Fragen diskutieren und/oder entscheiden müssen, werden von der landespezifischen Gesetzgebung bestimmt, und einer Verteidigungsstufe zugeordnet.

Der präventive Personenschutz

Die präventive Schutztätigkeit bedeutet die Mitwirkung an der Gewährleistung der persönlichen Sicherheit von geschützten Führungspersönlichkeiten aus dem Ausland. Hierbei konzentriert sich die landespezifische Sicherheitsbehörde in erster Linie auf die Aufklärung solcher Informationen, die die zu erwartende Sicherheitslage beeinflussen können, deshalb hängt diese Tätigkeit eng mit dem offiziellen Programm der Schutzperson und den entsprechenden Schauplätzen zusammen.

Verteidigungsstufen des permanenten Personenschutzes[6]

Die sogenannten Verteidigungsstufen für den permanenten Personenschutz werden gemäß der zu erwartenden Bedrohung bestimmt.

Die Verteidigungsstufen sind folgende:

I. Die schutzwürdige Person wird erheblich gefährdet, es wird mit einem Anschlag gerechnet und es liegen darüber konkrete, kontrollierte Informationen vor.

Den betroffenen Personen wird eine permanente Sicherheitsbegleitung zur Verfügung gestellt und es müssen alle Elemente des Systems des Personenschutzes angewendet werden.

II. Die schutzwürdige Person wird gefährdet, es wird mit einem Anschlag gerechnet und es liegen darüber nicht kontrollierbare Informationen vor.

Den betroffenen Personen wird eine permanente Sicherheitsbegleitung zur Verfügung gestellt und es müssen folgende Elemente des Systems des Personenschutzes angewendet werden: Vorbereitungsaufgaben, Objektschutzmassnahmen, Unterkunftssicherung, Verteidigung des Veranstaltungsortes, Marschsicherung.

III. Die schutzwürdige Person wird nicht gefährdet, aber Ihre Einstufung und die von ihr bekleidete Position in der Wirtschaft begründen eine permanente Sicherheitsbegleitung.

[6] Reinhard Scholzen: Personenschutz, Stuttgart, Motorbuch Verlag, 2004, Seite 45-46

Den betroffenen Personen wird eine permanente Sicherheitsbegleitung zur Verfügung gestellt und es müssen folgende Elemente des System des Personenschutzes angewendet werden: Vorbereitungsaufgaben, Objektschutzmassnahmen, Unterkunftssicherung.

Aufgaben der Personen des Personenschutzes[7]

- Kommandeur der Personenschützer: ist verantwortlich für die Arbeit der Personenschützer und leitet diese Tätigkeit den landesspezifischen Gesetzregelungen und Dienstvorschriften entsprechend. Er koordiniert und kontrolliert die Aufgaben der Personenschützer.
- Personenschützer des Veranstaltungsorts: er kontrolliert den aktuellen Veranstaltungsort, und gewährleistet, dass alle Sicherheitsmaßnahmen eingeführt werden. Er meldet dem Kommandeur der Personenschützer, ob es allfällige Probleme gibt oder nicht. Er koordiniert die Personenschützer in der äußeren Verteidigungszone8. Das gilt auch für die Unterkunftsicherung.
- Personenschützer9: er/sie ist klassischer Personenschützer, der/die die schutzwürdige Person persönlich begleitet. Der Personenschützer ist zuständig für das rechtzeitige Erkennen und Verhindern der Gefahren. Dabei wird besonders auf ungewöhnliche Gegenstände und Abläufe, auf allfälliges und/oder ungewöhnliches Verhalten von Personen geachtet.
- Sicherheitsfahrer10: Fahrer im privaten Personenschutz sind von Berufs wegen in besonderem Maße den Gefahrensituationen und dem Stress im Straßenverkehr ausgesetzt. Für ihre Trainings stehen speziell ausgebildete Moderatoren mit entsprechenden Trainingsprogrammen zur Verfügung. Die Trainings bestehen aus vier Hauptmodulen: Fahrtraining bei extremem Wetter, Antiterrorfahrtraining, taktische Ausbildung, Protokollkenntnisse.

Elemente des Systems des Personenschutzes
Vorbereitungsaufgaben

Die präventive Schutztätigkeit bedeutet die Mitwirkung an der Gewährleistung der persönlichen Sicherheit von geschützten Führungspersönlichkeiten aus dem Ausland[11]. Hierbei konzentriert sich das Wachregiment der Republik[12] und die Terrorabwehrzentrale in erster Linie auf die Aufklärung solcher Informationen, die die zu erwartende Sicherheitslage

---

[7] Reinhard Scholzen: Personenschutz, Stuttgart, Motorbuch Verlag, 2004, Seite 33-43
[8] oder den privatwirtschaftlichen Sicherheitsdienst
[9] Bodyguards
[10] Cheffahrer, Fahrer von Führungskräften
11 Bundesakademie für Sicherheitspolitik: Sicherheitspolitik in neuen Dimensionen, Bonn, Verlag Mittler & Sohn GmbH, 2001, Seite 347 - 609
12 Aus dem Grundauftrag des Wachregiments der Republik ergibt sich die Aufgabe, das Verüben gewalttätiger Handlungen (Angriffe) gegen ausländische und einheimische geschützte Personen zu verhindern. Das Wachregiment der Republik und die Terrorabwehrzentrale nehmen ihre Sicherungsaufgaben den Normen in den internationalen12 und nationalen12 Vorschriften entsprechend wahr.
Die UNO formulierte 1973 den Begriff der international geschützten Person. Darin wurden Prävention und Strafen von Verbrechen gegen geschützte Personen definiert. Diese Bestimmungen gelangten 1977 in die ungarische Rechtsordnung.
Das Wachregiment der Republik steht in direkter Verbindung mit den betreffenden Abteilungen des Außenministeriums und den partnerschaftlichen Sicherheitsorganen hinsichtlich der Vorbereitung und Abwicklung offizieller Besuche geschützter Personen im In- und Ausland.
Das Wachregiment der Republik und die Terrorabwehrzentrale erstellten zur Sicherung der ungarischen und internationalen geschützten Personen einen Plan, in dem das Sicherungssystem, sowie die Aufgaben der kooperierenden Sicherheitsorgane und Dienste den Schutzkategorien entsprechend definiert werden.

beeinflussen können, deshalb hängt diese Tätigkeit eng mit dem offiziellen Programm der Delegation und den entsprechenden Schauplätzen zusammen. Die im Durchführungsbereich der Sicherungsaufgaben tätigen Mitarbeiter des Wachregiments der Republik und der Terrorabwehrzentrale arbeiten mit den für die Abwicklung der Veranstaltungen verantwortlichen staatlichen oder zivilen Protokollorganisationen zusammen und darüber hinaus auch mit den Mitarbeitern sonstiger Organisationen, die an der physischen Sicherung beteiligt sind, sowie den Mitarbeitern der ausländischen Partnerdienste.

OBJEKTSCHUTZMASSNAHMEN

Der Objektschutz umfasst bauliche, technische und organisatorische Maßnahmen zum Schutz und zur Verteidigung von Objekten generell, sowie von einzelnen Bereichen mit besonderen Sicherheitsanforderungen (die geschützten Personen, wichtige und/oder besonders wertvolle Einrichtungen, Veranstaltungsorte) gegen alle schädlichen Einwirkungen.

Es soll erreicht werden, dass mit einem betriebswirtschaftlich vertretbarem Aufwand ein unerlaubtes Eindringen von Personen oder das gewaltsame, schädliche Einwirken von außen ohne größeren Zeitaufwand und ohne rechtzeitig entdeckt zu werden, verhindert wird.

Sicherstellen einer integrierten Planung

Objektschutzvorhaben sind gemäß den in der Gesetzgebung festgelegten Projektschritten und Genehmigungsverfahren zu realisieren.

Die Anordnung von Objektschutzmaßnahmen wird auf Basis der Sicherheitskonzepte vom Aufklärungsdienst festgelegt. Der Aufklärungsdienst ist über entsprechende Vorhaben rechtzeitig zu informieren und in die Planungsunterstützung einzubeziehen.

Spezielle Objektschutzmaßnahmen sind ab mittlerem Bedrohungsgrad, z.B. für betriebswichtige Versorgungs- und Entsorgungssysteme, Kommunikationssysteme, Rechenzentren und Datenarchive, sowie Aufbewahrungsorte von größeren Bargeldbeträgen, wertvollen Rohstoffen oder Betriebsmaterialien (Kritische Infrastruktur) zu treffen.

Unterkunftsicherung

Hierzu gehört die Gesamtheit der durch die Wohnungssicherungsgruppe laufend angewandten Sicherheitsregeln am Wohnort der geschützten Person, mit denen die Beobachtung, Aufklärung, Durchsuchung von Sendungen, Neutralisierung von Angreifern und Rettung der geschützten Person(en) sichergestellt werden kann.

Die Basis für den Unterkunftsschutz bilden die Methoden des Objektschutzes.

Bei der Auswahl der Unterkunft sind die fachprotokollarischen Gesichtspunkte zu berücksichtigen, die mit dem für die Sicherheit der geschützten Person verantwortlichen Organ abzustimmen sind.

Die Sicherung der Unterkunft am Unterkunftsort der geschützten Person beginnt noch vor ihrem Eintreffen und dauert bis zu ihrer Abreise.

Sicherung der Veranstaltungsorte

Die Sicherung von Schauplätzen ist die Gesamtheit von Ordnungsregeln, Maßnahmen und Tätigkeiten, die im Interesse des störungsfreien Ablaufs des gegebenen Ereignisses sowie der persönlichen Sicherheit der Teilnehmer und des Vermögensschutzes angewendet werden.

Ziel der Sicherung des Schauplatzes ist es, den ungestörten Ablauf der Veranstaltung sicherzustellen und die auf eine Ordnungsstörung gerichteten Bestrebungen zu unterbinden.

Dabei geht es um das Herausfiltern von auf eine Ordnungsstörung abstellenden Personen, die Isolierung dieser Personen in Zusammenarbeit mit den Polizeiorganen, das Fernhalten unbefugter Personen, sowie die Gewährleistung der körperlichen Unversehrtheit der an der Veranstaltung teilnehmenden, geschützten Führungspersönlichkeiten.

Aufgabe der den Ort sichernden Kräfte ist es, die Planung und Organisation der Sicherung des Schauplatzes zu unterstützen, sowie beim Auftreten eventueller Ereignisse die geplanten Sicherheitsmaßnahmen zu ergreifen. Der Kommandant für die Sicherung des Schauplatzes hat zu kontrollieren, ob der betreffende Ort geeignet ist für das Auftreten der geschützten Personen. Er informiert den Kommandanten des Personenschutzes über auftretende Probleme bzw. nimmt mit seinen Kräften während des Aufenthalts der geschützten Person am Schauplatz eine indirekte Sicherung in der äußeren Schutzzone vor.

Ein wichtiges Element der Sicherung des Schauplatzes ist die pyrotechnische Durchsuchung des Ortes, die sich auch auf das Bedienungspersonal[13] sowie auf eine Durchsuchung der Teilnehmer und der Gäste erstreckt.

Die Sicherung des Schauplatzes beginnt einige Stunden vor dem Eintreffen der geschützten Personen und dauert bis zum Ende des Aufenthaltes der geschützten Personen am Ort des Geschehens.

Marschsicherung

Die Anreise zu den Programmorten und den Unterkünften geschieht in den meisten Fällen mit Pkw. Zur Durchführung der Sicherung der Reisen ist die Ausgestaltung einer entsprechenden Fahrzeugflotte, sowie eines Personalbestands an Monteuren und Wartungsmechanikern erforderlich.

Der Fahrzeugkonvoi wird durch den Kommandanten der Personensicherung zusammengestellt und gesteuert.

Das erste Fahrzeug ist das Polizeigeleitfahrzeug, das den anderen Verkehrsteilnehmern anzeigt, dass hier eine geschlossene Fahrzeugkolonne auf einer bestimmten Strecke verkehrt und sekundär die Strecke auskundschaftet. Auf das Geleitfahrzeug folgt das Protokollfahrzeug mit den für die Organisation verantwortlichen Personen. Dem Protokollfahrzeug folgt ein Sicherheitsfahrzeug.

Die Schutzeigenschaften des Fahrzeugs des Hauptgastes werden in Abhängigkeit von der Stufe des Schutzes bestimmt. Auch der mögliche Einsatz eines Reservefahrzeugs wird durch ebendiese Einstufung des Schutzes bestimmt.

Auf das Fahrzeug des Hauptgastes folgt ein weiteres Sicherheitsfahrzeug.

Die Kolonne wird durch ein Polizeifahrzeug zum Abschluss des Konvois gedeckt.

Sonderschutzfahrzeuge[14]

Die mit besonderen Panzerungen versehenen Fahrzeuge werden in verschiedene Schutz- bzw. Schussfestigkeitsklassen eingestuft. An dieser Stelle sollte angemerkt werden, dass sich diese Schutzfähigkeiten nicht immer auf das ganze Fahrzeug erstrecken, sondern damit die Schutzfähigkeit der eingesetzten Materialien gemeint ist. Die Sicherheitsstufen werden nach

13 STAFF= CREW

14 www.audi.de , www.mercedes.de , www.bmw.de , (Heruntergeladen: 02.05.2011)

DIN15 und Euronorm16 klassifiziert, je nachdem, welchen Waffen die Panzerung standhält. Für „durchsichtige“ Materialien (Glasscheiben) gilt die Norm EN 1063, für nicht „durchsichtige“ Materialien (Karosserieelemente) gelten die normen EN 1522 und EN 1523.

Die Prüfung der Fahrzeuge wird beispielsweise in Deutschland durch spezielle Waffenprüfinstitute vorgenommen. Die Einstufungen beziehen sich von VR1 bis VR7 auf die Karosserieelemente, und analog dazu lassen sich auch für die verglasten Elemente die Stufen VR1 bis VR7 vergeben. In breiten Kreisen angewandte Einstufungen sind VR4 und VR6/VR7. Der Schutzgrad bedeutet bei den sogenannten schwer gepanzerten Fahrzeugen, dass die Karosserie der Einstufung VR7 und die Verglasung der Einstufung VR6 entspricht. Selbstverständlich halten derartige Fahrzeuge nicht nur dem Feuer aus klassischen Feuerwaffen stand, sondern auch Explosionen, heftigen Schlägen, Spannungen und Brandbomben (Molotowcocktail)17.

Gesundheitssicherung

Die Gesundheitssicherung wird vom Staatlichen Rettungsdienst durchgeführt. Die Anwesenheit der daran beteiligten Rettungsoffiziere, Fachärzte, Pfleger und Rettungsfahrer ist nur an den Veranstaltungsorten erforderlich. Der Dienst wird mit den geltenden Vorschriften entsprechend ausgerüsteten Rettungs- und Notoperationsfahrzeugen getan. Im Rettungs- und Unfall- bzw. Notoperationswagen müssen sämtliche Mittel, Medikamente, Verbandszeug, Bruchschienen, bzw. zur Wiederbelebung notwendigen medizinischen Geräte zur Verfügung stehen, um gegebenenfalls auch mehrere Patienten versorgen zu können. Die bei unseren Veranstaltungen versorgten Patienten müssen bei Bedarf mit eigenen Rettungseinheiten ins Krankenhaus oder an weitere Versorgungsstellen geliefert werden, mit denen vor Beginn der Sicherung der Kontakt aufgenommen werden muss und die über die etwaige Einlieferung von Patienten in Kenntnis gesetzt werden müssen.

Brandverhütung und technische Hilfe

Während der Escortfahrt werden die Feuerwehr- und technische Hilfstätigkeiten die ausgebildeten Sicherheitsfahrer durchführen, bis zur Ankunft der staatlichen Feuerwehr und des Rettungsdienstes, z. B.:

[15] Deutsches Institut für Normung e.V.
[16] Europäische Norm
[17] Die Bezeichnung *Molotowcocktail* verwandten während der Zeit des „Winterkrieges” in Finnland erstmals finnische Soldaten für die gegen sowjetische Panzer eingesetzten Wurfbrandsätze. Die finnische Armee verfügte nicht über ausreichende Mengen an Panzerabwehrgeschossen gegen die Übermacht der sowjetischen Panzerverbände, weshalb sie zu dieser einfachen Waffe griff.

Spezielle Ausstattungen:

- Blaulicht und Sirene
- Funk- und andere Kommunikationssysteme
- 1 Stk. 6 kg Trockenlöscher + 5 kg CO_2
- Löscher
- „Force" Feuerwehrachse + Sicherheitsgurt-Schneider + andere Rettungswerkzeuge + Taschenlampen + Warnweste
- 3 Stk. Verbandtaschen

Die Veranstaltungsorte sollten mit entsprechenden Brandmeldern und Brandschutzeinrichtungen ausgestattet werden.

Lebensmittelkontrolle

Die ausgebildeten Personen sind für die Lebensmittelkontrolle zuständig und überwachen, dass die Vorschriften des Lebensmittelgesetzes (Schutz der Konsumentinnen und Konsumenten vor gesundheitlichen Gefährdungen und Täuschungen, Sicherstellung des hygienischen Umgangs mit Lebensmitteln) eingehalten werden.

Der Hersteller ist für deren Qualität und Kennzeichnung selbst verantwortlich und muss im Rahmen seiner Tätigkeit mit einer geeigneten Selbstkontrolle dafür sorgen, dass seine Lebensmittel den Vorschriften entsprechen und sie - soweit nötig - untersuchen lassen.

Logistische Aufgaben

Die Ausstattung des Personalbestands ist schon während der Planung und Durchführung der Tätigkeiten von herausragender Bedeutung, doch der Umstand, mit welchen Mitteln, Ausrüstungen und technischen Instrumenten die Aufgabe durchgeführt wird, ist die Kernfrage.

Zum Themenkreis der Ausstattung gehört, mit welcher Bekleidung (Winter-, Sommer- oder wasserabweisende Kleidung, Gewicht, etc.), mit welchen Waffen (Kaliber, Visiervorrichtung, Gewicht, etc.) und mit welcher Art von kugelsicheren Westen (Brust, Nacken, Gesichtsschutz, Gewicht, etc.) der Personalbestand versorgt wird.

In der Aufzählung lässt sich keine einzige Materialart hervorheben, weil jedes Mal die konkrete Einsatzsituation entscheidet, was wichtig und was am wichtigsten ist. Es kann sich die Möglichkeit ergeben, dass Dinge wichtig werden, die wir auf der Grundlage der vorherigen Bewertungen als zu vernachlässigend ansahen.

Es genügt nicht, dass die für den Personalbestand benötigten Mittel und Materialien nur vorhanden sind, es ist ebenso wichtig, dass das Material dem Personalbestand am richtigen Ort, zur richtigen Zeit in der entsprechenden Menge und Qualität zur Verfügung steht.

Die Ausstattung des Personalbestands bezieht sich über die Materialien hinaus auch auf die Dienstleistungen.

Reserve

Der Wartungsdienst und/oder die Wartungsmannschaft müssen sich in der Werkstatt auf die Ausführung von mobilen Problembehebungsaufgaben und Kleinreparaturen vorbereiten, und müssen über die zur Ausführung der Aufgaben nötigen Ausrüstungen, Reparaturutensilien und Vorräte verfügen.

Ordnung der Leitung und Führung

Die Leitungsordnung der Sicherheitsbegleitungsaufgaben wird gemäß den gültigen landespezifischen Gesetzen und den inneren Dienstvorschriften bestimmt. Dementsprechend wird der Kommanduer des Personenschutzes unmittelbar dem diensthabenden Offizier der Sicherheitsbehörde berichten, wenn staatliche Schutzpersonen betroffen sind. Der kontinuierliche Kontakt mit der Zentrale des betroffenen Lagezentrums18 wird durch EDR19, UKW und per Handy gewährleistet.

Literaturverzeichnis

[1] Koran (75:7-10)

[2] Reinhard Scholzen: Personenschutz, Stuttgart, Motorbuch Verlag, 2004

[3] Bundesakademie für Sicherheitspolitik: Sicherheitspolitik in neuen Dimensionen, Bonn, Verlag Mittler & Sohn GmbH, 2001

[4] János PATAKI – Péter SULÁNYI : LAGE- UND ANALYSEZENTRUM bei einem internationalen Unternehmen, Abhandlung, Militär-Ingenieur, Budapest, 2011

[5] www.audi.de (Heruntergeladen: 02.05.2011)

[6] www.mercedes.de (Heruntergeladen: 02.05.2011)

[7] www.bmw.de (Heruntergeladen: 02.05.2011)

[18] Situation Centre = Sicherheitszentrale + Krisenmanagement Situations Centre(SitCen). Das SitCen erhielt eine wichtige Aufgabe auf dem Gebiet der Bedrohungsbewertung, denn es geht nun darum, jene Fähigkeiten zu entwickeln, die sich für eine Analyse und Bewertung der globalen Anforderungen eignen.
Das SitCen wird rund um die Uhr an allen sieben Tagen der Woche betrieben. Egal an welchem Punkt der Welt ein Ereignis, eine Katastrophe und/oder anders geartete Gefahrensituation eintritt, die Mitarbeiter im SitCen halten die Informationen fest und erfüllen gleichzeitig damit ihre Alarm- und Berichtspflicht. Auf der Grundlage der zur Verfügung stehenden Informationen können sie entscheiden, welche Organisationen die Informationen betreffen bzw. interessieren könnten. Informationsquellen können die verschiedenen maßgeblichen Nachrichtenportale sein. Natürlich kann unter Umständen auch der Einsatz von Übersetzern notwendig sein, wenn für das Verständnis der Nachrichtenquelle eine fachgerechte Übersetzung benötigt wird. Deshalb ist es unvermeidlich, dass für diese Personen ein Bereitschaftsdienst angeordnet wird. Die wichtigen Informationen sind sofort weiterzuleiten. Dem SitCen stehen sämtliche Kommunikationskanäle (Telefon, Fax, E-Mail, Radio) zur Verfügung. Selbstverständlich dürfen die sensiblen Informationen nur auf kodierten und/oder geschützten Leitungen weitergereicht werden.

[19] Einheitliche Digitales Funknetz

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Venekei József
venekei.jozsef@zmne.hu

FIRST HAND EXPERIENCES OF THE MULTINATIONAL LOGISTICS TRAINING PROGRAM MAGLITE 2011/1

Absztrakt/Abstract

A MAGLITE 2011/1 Multinacionális Logisztikai Képzési Program 2011 júniusában került végrehajtásra öt nemzet, köztük Magyarország, Egyesült Királyság, az Egyesült Államok, Hollandia és a Cseh Köztársaság tisztjeinek bevonásával. A képzési programnak első ízben adott helyet a Magyar Honvédség Központi Kiképző Bázisa Szentendrén. A júniusi gyakorlat tartalmát és koncepcióját tekintve új kihívások elé állította a gyakorlaton résztvevő magyar tiszti munkacsoportot. Cikkemben összegzem a gyakorlat végrehajtásának főbb tapasztalatait és azokat a lehetőségeket melyek a jövőben tovább segíthetik a gyakorlat sikeres végrehajtását.

The exercise organised within the framework of the MAGLITE 2011/1 Multinational Logistics Training Program was conducted in June 2011 with the participation of five nations: Hungary, The United Kingdom, the United States, Netherland and the Czech Republic. The Training Program first time was held at the Central Training Base of HDF in Szentendre. The exercise with its content and operational design approved itself as a great challange for the hungarian officers' syndicate. In my article I'm going to summarize the lessons learned from the exercise and describe the possibilities which may improve its succesful execution in the future.

Kulcsszavak/Keywords: *MAGLITE, Logisztikai képzési program, Összhaderőnemi logisztikai műveletek ~ Logistics training program, Joint Logistics Operations*

PRELIMINARY STEPS OF THE EXERCISE MAGLITE

First part of the Multinational Logistics Training Program MAGLITE 2011/1 was conducted in June 2011 at the Central Training Base of HDF1 in Szentendre with participation of five nations: Hungary, The United Kingdom, The United States, Netherland and The Czech Republic.

The exercise MAGLITE is based upon the Joint Logistics Operations Course (JLOC) organized for the senior officers of the Army, Navy and Air Force in Deepcut by the Defence Logistics School. Though JLOC organized mainly for the British officers nowadays it is getting more international due to the ivitations of the Defence Logistics School. MAGLITE is traditionally held in Hungary year by year where the officers studying at the Department of Military Logistics joining the British syndicates can get knowledge of operational level military decision making process in the field of military logistics. MAGLITE also provides a good opportunity for them to improve their language skills and get some experience of common work.

In April 2011 Lt Col Réger (Ret) and myself arrived to Deepcut to attend a coordination meeting organized by the British party. During the planning meeting we were introduced by our partner from the British Distaff2 Major Shakespeare with the new operational scenario, the joint operational area (JOA) and the size and compound of the British contingent taking part in the operation. Due to the significant changes in operational scenario we had to reconsider the size and role of our contingent which would take part in operation. Since the British side wanted to adopt a finished operational scenario from their PJHQ3 we had to made a compromise with the British Distaff and give up our plans regarding the operational scenario and mission.We tried to find different solutions to the problem how we can enable Hungarian officers into the common work.We faced the problem again, that we can't involve into the task a brigade strong organization supported by Air Force elements which would allow to carry out an operational level logistic planning work. By the end of the meeting we agreed to deploy alltogether three light armoured infantry battalion strong multinational contingent to the area of operation as a force protection element for the British logistic troops and their necessary military assets to enable the UN4 and NGO5's effort to alleviate the current Humanitarian Crisis and provide C26 logistic functionality to the UN and NGOs.

After arriving home the Military Logistic Department immediately started its direct preparation for the exercise.

The preparational period of the exercise was complicated due to the fact, that our University in its today situation has been not able to accomodate the 50 member strong participants thus a decision has been made to move the exercise to the Central Training Base of HDF in Szentendre. The exercise leader also made a right decision when he created a staff including officials from different organizations of the University that made the work much easier for the Department of Military Logistics. According to my experiences a good cooperation was developed amongst the people who were involved into the preparation and execution of the exercise. The common work between the University and the Central Training Base of HDF proved to be an exemplary cooperation.

[1] Hungarian Defence Forces
[2] Directors' staff
[3] Permanent Joint Headquarter
[4] United Nations
[5] Non Governmental Organization
[6] Command and control

1. picture. Staff meeting in Szentendre
photo made by Dr. József Varga

EXECUTIONAL PERIOD OF THE EXERCISE

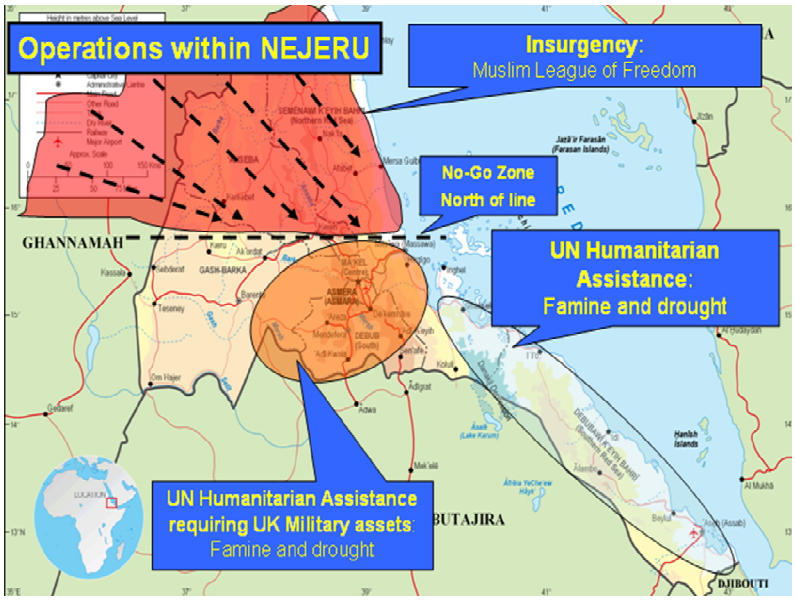
The Operational Area of the exercise was in Nejeru, a fictitious state in north- eastern part of Africa. There are famine and drought in Nejeru, thus several UN and NGO's are operating in the eastern part of the country trying to provide humanitarian assistance to local citizens.

The situation is complicated by the fact, that they are limited by the numbers of vehicles and logistic assets in country and requests for assistance from the NEJERU Defence Forces (NDF) to provide assistance with aid distribution have been refused and the northern part of the country is controlled by a hostile organization called Muslim Legue of Freedom (MLF). NDF as directed is defeating the Muslim rebellion of the Muslim League of Freedom and see the humanitarian problem as something that should be left to others to deal with.

The UK forces's mission was to conduct operations in the NEJERU JOA7 which would include the offload and distribution of designated UK equipment and aid from SPOD8s and APOD9s and also to provide military support to the UN (and designated NGOs) to enable the distribution of humanitarian aid within JOA. In need they had to be prepared to offer C2 logistic functionality to the UN and NGO organisations and support the maintenance of secure LoC[10]s and logistic hubs within JOA, in order to create the conditions within NEJERU for the attainment of the MSTP [11]as part of the wider cross government stabilisation plan.

In the initial period of the exercise we had to make some serious changes in the scenario. After the staff briefing of the British Distaff it became clear, that in paralell with their logistic forces the British side is about to deploy significant combat and combat service elements in the JOA. This unexpected step hase made unnecessary for the multinational brigade to deploy three of its infantry battalions which would have attached to the british logistic forces as a force protection element. According to the fast decision of the Hungarian Distaff the organizational structure of the multinational contingent has been changed.

[7] Joint Operational Area
[8] Sea Port of Disembarkation
[9] Air Port of Disembarkation
[10] Line of Communication
[11] Military Strategic Transition Point



2. picture. Operational area in Nejeru (EXCON slide pack 2011, DCLPA)

A MILU12 has been created with its own NSE13 and an infantry battalion strong force protection element. In our conception a water purification platoon supported by transport subunits which were integrated into the structure of a MILU would have supplied the designited for them refugee camp. This concept was discussed with the British exercise leader who went along with us. Surprisingly from the datas were sorted out later on by the British Distaff became clear, that the UN organizations had got an enormous stockpile of water in the area enough to supply all of the refugee camps situated on the territory of Nejeru. They also had the needed transport assets for distribution. All of these missunderstandings came from the fact, that the British Distaff didn't share with us the exercise documents, and we were introduced with them in the time only when they were sorted out. Despite all of theese facts we can state that Hungarian officers who were involved in the MAGLITE exercise solved their planning tasks in very flexible way.

3. picture. Syndicate work
Photo made by Dr. József Varga

LESSONS LEARNED FROM THE EXERCISE MAGLITE 2011/1

[12] Multinational Integrated Logistic Unit
[13] National Support Element

- Preparation for the exercise MAGLITE 2011/1 was a model and elicited universal admiration of the British side.
- Cooperation between the University's and the Central Training Base's staff was exemplary, without any friction.
- IT[14] infrastructure and network provided by our University for the period of the exercise has proved its efficiency and contributed to the success of MAGLITE considerably.
- The infrastructure, catering service provided by the Central Training Base of HDF have fulfilled our hopes and had been praised by the British side.
- The level of proffesional knowledge of our MSc officers met the requirements but their language skills have to be improved so they can understand the native english speech. In my opinion NATO STANAG 3.3.3.3 should be the entrance level to take part in MAGLITE.
- Map work (electronic, paper) during the exercise has to be improved significantly. Practically I haven't found any datas on the map, including friendly, neutral and enemy forces' situation, LoCs, etc.
- In the preparational period MSc officers have to be introduced with the tactical and also the operational level MDMP[15] which have to be the frame for their planning work.
- Conception of the British exercise leader to form only one Hungarian syndicate working parallel with four British syndicates turned out faulty, because one planning team cannot interact with each of them and take into consideration their two or three COA[16]s during the planning work. Althoug there were LO[17]s included in each british syndicate, the cooperation depended only on COA has been choosen by the British side. There were British syndicates who had no interaction at all with the Hungarian planning team.

To solve this problem we have to consider 2 to 3 Hungarian MSc officers to be attached to each JLOC18 planning syndicate. Then each syndicate has its own HU syndicate to interact with. This way the Hungarian syndicate would have a need to articulate their timelines and STRAT lift 19needs to the JLOC syndicate to have some friction.

- The other solution could be to have a completely independent task created by the Hungarian Distaff which would be universal and would not depend on any British operational scenario but combined enough to have frictions with the British Syndicates regarding the deployment, APODs, SPODs, RSOM[20] tasks etc.
- According to my experiences gained in last three years I can state that the British Distaff shares the detailed task with us only in last moment or during the executional period of the exercise which doesn't allow us to prepare our officers, and leads to the described above complications that is why comletely unacceptable for us. If we are taking into consideration the fact that before the exercise the British participants have a one week long preparation within the framework of JLOC, we start the exercise under the unequal conditions and our role is reduced only for an assistance.

[14] Information Technology
[15] Military Decision Making Process
[16] Course of Action
[17] Liaison Officers
[18] Joint Logistic Operations Course
[19] Strategic Air Lift
[20] Reception Staging and Onward Movement

CONCLUSION

Multinational Training Program MAGLITE is playing very important role in the educational process of the Miklós Zrínyi National Defence University. It prepares the MSc officers to solve logistic planning tasks on operational level and learn the steps and content of the MDMP which role is nowadays fading away during the staff work.

Although there are some missunderstandings and differences of opinion with our British partner, we have to keep on working and developing MAGLITE which has a key position in the educational process of the Department of Military Logistics.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Venekei József
venekei.jozsef@uni-nke.hu

LESSONS LEARNED FROM THE EXECUTION OF THE MULTINATIONAL LOGISTICS TRAINING PROGRAM FOURLOG 2011

Absztrakt / Abstract

A Fourlog 2011 Többnemzeti Logisztikai Képzési Program 2011. május 01-13-ig került végrehajtásra az Osztrák Szövetségi Hadsereg bécsi logisztikai iskolájának, a Zrínyi Miklós Nemzetvédelmi Egyetem Hadtáp, Pénzügyi és Közgazdasági Tanszékének és a cseh Védelmi Egyetem hallgatóinak bevonásával. A képzési program elsődleges célja az volt, hogy felkészítse a résztvevő hallgatókat a béketámogató műveletek során, többnemzeti törzsekben várható szakfeladataik ellátására. A foglalkozások során a tisztjelöltek megismerték és gyakorolták a harcászati szintű katonai döntéshozatali mechanizmus lépéseit és a külföldi szaktisztekkel való együttműködés problematikáját. Cikkemben a képzési program tapasztalatait szeretném összegezni kihangsúlyozva annak pozitív és negatív oldalait és a program továbbfejlesztésének irányait.

The Multinational Logistics Training Program Fourlog 2011 was held from 01 to13 May 2011 with the participation of the cadets of the Logistic School of the Austrian Armed Forces in Vienna, the cadets of the Department of Supply, Finances and Economics of the Miklós Zrínyi National Defence University, and the cadets delegated to the exercise by the Czech Defence University in Brno. The primary aim of the training program was to prepare the participating cadets to work in multinational teams and perform their special tasks in peace support operations. During the lessons the cadets were familiarized with the steps of the tactical level Military Decision Making Process and the problematics of cooperation with the supply officers serving in foreign armies. In my article I would like to give a summary of the lessons learned from the training program Fourlog 2011 highlighting the positive and negative sides and to describe the directions of its possible development.

Kulcsszavak/Keywords: *Fourlog, Többnemzeti Logisztikai Képzési Program, Béketámogató művelet ~ Multinational Logistic Training Program, Peace Support Operation*

INTRODUCTION

The Multinational Logistics Training Program Fourlog 2011 was held from 01 to 13 May 2011 with the participation of the cadets of the Logistic School of the Austrian Armed Forces in Vienna, the cadets of the Department of Supply, Finances and Economics of the Miklós Zrínyi National Defence University and the cadets delegated to the exercise by the Czech Defence University in Brno.

The task of the Hungarian, Czech and Austrian cadets was to take part in a peacekeeping training program in Austria, and in the role of G4 to carry out robust logistic planning work regarding the supply tasks of the peacekeeping brigade in Hungary, to deploy the functional elements of the logistic battalion and as a new element, to practise the S4 tasks of the deployed NSE (National Support Element) in the Czech Republic.

The cadets trained in the field of finances were also involved in the execution of the tasks, carrying out a series of financial planning, and playing the role of a financial officer of the national contingent.

It was also a new element in the exercise that during the Hungarian phase of the exercise the whole contingent of Fourlog took part in a night orientation march supported by GPS in the exercise area of the MZNDU (Miklós Zrínyi National Defence University).

SHORT PRESENTATION OF THE FOURLOG[1] MULTINATIONAL LOGISTICS TRAINING PROGRAM

Fourlog is a tactical level multinational logistics training program, the primary aim of which is to prepare the cadets of the participating nations for the special supply tasks during a peace support operation (PSO) in multinational logistic teams.

In the process of planning and execution they have to use all of their theoretical and practical knowledge learned during the time of preparation for the exercise.

The fictitious scenarios of the Fourlog exercise are based upon a fictitious PSO (Peace Support Operation) with UN (United Nations) mandate. The training program uses real geographic objects with fictitious states, borders and population.

The training program is held yearly and consists of the following three phases:

- Preparation for the PSO in Austria taking part in a practical peacekeeping training;
- Logistic reconnaissance of the OA (Operational Area) and logistic planning of the tasks of the PSO in Hungary;
- Site survey of the area of deployment of the logistic battalion's subunits and NSE as well as practicing the tasks of convoy protection in the Czech Republic.

The Fourlog Logistics Training Program is supervised by the co-directors and led by the national commanders appointed in each country by the co-directors. In the period of the exercise the work of the multinational syndicates is supported by the teachers from each nation.

[1] The name of the training program comes from a pun referring to the four nations that used to take part in it solving mainly special logistic tasks. At present there are only three participating nations, but the name remained the same. On the other hand Fourlog can be understood as „For Logistics".

1. picture. Logo of Fourlog
Designed by J. Venekei in 2004.

3. DESCRIPTION OF THE PHASES OF FOURLOG 2011

In the first phase of the exercise, cadets took part in a practical preparation for the PSO in Vienna. After staff briefing and examination of the Brigade Commander's Frego (Fragmentation Order) the syndicates started their work with the tactical level MDMP (Military Decision Making Process).

During the preparation they visited the Bundesheer's[2] 33rdInfantry Battalion in Grossmittel where they had a series of theoretical classes about the structure and operation of mobile and static checkpoints and the rules of radio communication in the OA.

In the practical part of the preparation they learned how to deploy and operate the battalion's ammunition, food and fuel supply points. Additionally they were prepared for the tasks of mine awareness including mine disposal.

2. picture. Grossmittel, Demonstration of the Food Supply Point
Photo made by the author

During the second phase of the exercise, the staff that took part in the exercise redeployed to Hungary. After the situation report, the syndicates immediately started their preparation for the logistic reconnaissance of the OA. Four local governments (Veresegyház, Mogyoród, Gyál, Vecsés) with the support of the Defence Committee of Pest County were involved in

[2] German name of the Austrian Armed Forces

this task, in which the cadets, using their recce checklist, tried to get the information about the supply possibilities and facilities and also studied the tasks of HNS (Host Nation Support).

At the same time the preparatory group of the Peacekeeping Brigade carried out their site survey in Szolnok, where they visited the 86th Szolnok Helicopter Base which was designated as a possible APOD (Air Port of Disembarkation). They also visited the Szolnok Industrial Park which was considered as the area of deployment for the Logistic Battalion of the Brigade.

After the logistic reconnaissance the syndicates, according to the given task, started their planning the air and rail deployment of the Peacekeeping Brigade to OA using the ADAMS [3] system. They made the calculation of the class V. material for a long distance march, and prepared a detailed supply plan for the refugees arriving in the area of responsibility of the peacekeeping brigade.

Cadets trained in the field of finance made a calculation for the allowances of the personnel taking part in the mission, prepared the plan of means and practised the NATO rules of billing.

3. picture. Budapest, Syndicate work
Photo made by the author

In the final part of the second phase syndicates got the task to explore the route of redeployment to the new area of responsibility, and draw up a plan for the convoy protection of the peacekeeping brigade. The Hungarian phase of the training program ended with the syndicates delivering their reports in an open session.

In the third phase of the exercise, after redeployment to Brno, according to the new task of the peacekeeping brigade, the syndicates started their direct preparation for the logistic reconnaissance of the new area of deployment.

Relying on what they learned from the recce, the cadets in the role of the commander of a logistic subunit have planned the deployment and operation of the logistic support elements of a battalion.

After the planning work, on the next day the cadets took part in tactical training in the training centre of the Czech Army in Vyskov. According to a fictitious situation, the cadets in the role of platoon commander practised setting up and securing a transport column and repelling various hostile acts against the transport column using modern simulation systems,

[3] Allied Deployment and Movement System

such as Miles 2000. During the execution of this task the participating cadets were also trained in CASEVAC (casualty evacuation) procedures.

The simulation systems, transport and supply vehicles and the infantry platoon which were provided by the Training Centre of the Czech Army allowed for us to organize a really successful and effective practical training exercise in the field.

4. picture. Vyskov, Operation of the Refuelling Point
Photo made by the author

LESSONS LEARNED FROM FOURLOG 2011

After the evaluation of the execution of Fourlog 2011, the following positive lessons were learned:

- The objectives of the Multinational Logistics Training Program were fully achieved;
- The special tasks carried out during the exercise provided an excellent opportunity for the participating cadets to prepare for working on tours of duty abroad;
- The junior cadets who took part in the training program gained useful experience in carrying out international tasks, which promotes the effective execution of the next Fourlog program;
- In the period of the immediate preparation and execution of the training program the participants' confidence has increased and their language skills, including their technical vocabulary, have improved dramatically;
- The training program included a wide range of special knowledge the acquisition of which is only possible in an international environment;
- The Hungarian cadets used the LOGFAS[4] system confidently due to the competent preparation prior to the execution of Fourlog 2011.

Since its birth the FOURLOG Multinational Logistics Training Program has become a large and complex logistic exercise, which is being developed continuously by the teachers and instructors of the participating nations. The co-directors and national commanders from

[4] Logistics Functional Area Services. NATO's primary automated logistic systems are packaged within LOGFAS under the Automated Command and Control Information System (ACCIS). LOGFAS is currently a functional prototype comprising the Logistic Database (LOGBASE), the Allied Deployment and Movement System (ADAMS), the Allied Commands Resource Optimisation Software System (ACROSS), and the Logistic Reporting System (LOGREP).

each nation meet twice a year before the exercise to review the incoming tasks and find the possibilities of the improvement of the exercise scenario and logistic tasks. According to this, in 2011 we also included the National Support Element in the scenario. It proved to be a good decision, because this way the participating cadets got a detailed picture about the supply chain and the problems involved in supporting our troops thousands of kilometres away from the home bases.

From previous exercises it became obvious that the Operational Scenario was hard to understand and it had lots of unnecessary information, thus our cadets were confused and got lost in details. In order to make it possible for them to understand it better and improve our cadets' general military training, in 2011, for the first time in the history of the exercise we introduced the 1st and 2nd steps of the tactical level MDMP as a new element. In the first phase of the exercise in Vienna after receiving the Operational Scenario and the Brigade Commander's Frego, each syndicate had to review the situation and carry out the mission analysis. It proved to be an effective way of making sure that the syndicates understood the situation and the essence of the fictitious PSO.

The next problem we are facing year by year is that the cadets have to work and report in different roles. The exercise instructions vary from exercise to exercise, cadets have to complete G4 and S4 level tasks, which can be confusing and sometimes it requires an abstract way of thinking. In the next years this problem can be solved by reducing the task levels. It is necessary because of the fact that the training of the cadets of each nation is different.

While the Hungarian and Czech cadets are trained to solve both S4 and G4 level logistic tasks, the Austrians are prepared for S4 level tasks only.

There is no doubt that the biggest challenge during the exercise is the application of LOGFAS. Two years ago we recognized the necessity of LOGFAS, therefore since last year it has been included in our curriculum. Because of the lack of such type of preparation, the Austrian and Czech cadets couldn't be involved in the planning tasks based on the application of LOGFAS. To bring foreign cadets to the same level, from 2012 Hungarian teachers will deliver a course in Austria and the Czech Republic in the period of preparation.

CONCLUSION

Fourlog itself is a definitive point in the educational process of the Miklós Zrínyi National Defence University. It prepares the cadets how to carry out a tactical level planning work in multinational teams gathering essential information about the planning, setting up and running an operation abroad.

Nowadays our University is going through a definitive change. The whole educational process is going to be changed as well but we have to keep on working and developing Fourlog which is playing important role in education of the cadets trained in the field of military economics.

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Horvayné Fehér Judit
feherjenator@gmail.com

A RENDŐRSÉG INFORMATIKAI BIZTONSÁGI STRATÉGIÁJA ALAPJAINAK MEGHATÁROZÁSA

Absztrakt

A Magyar Köztársaság Testületi Stratégiájában megfogalmazott céloknak megfelelően „a stratégia strukturálisan sajátos kettős karakterű célhierarchia: minden egyes cél úgy is felfogható, mint egy másik, magasabb rendű cél elérésének eszköze. Ez sajátos cél-eszköz piramis formájában érzékelhető, melyben a céljelleg a piramis csúcsa felé, az eszköz jelleg pedig a talapzata felé erősödik. Legfontosabb elemei a stratégiai célok, amelyek a rendőrség testületének jövőre vonatkozó legfontosabb törekvéseit foglalják össze, valamint a cselekvési sávok, amelyek a stratégiai célok megvalósításának jól körvonalazható szegmensei, amelyek az adott cél megvalósítása irányába ható, logikailag összetartozó feladatokat, feladatcsomagokat foglalnak magukba.” Ennek tükrében a rendőrség informatikai biztonsági stratégiája azon jövőbeni állapotjellemzőket kell, hogy fogalmazza meg, amelyeket a legfontosabbnak tartunk és hosszabb távon el kívánunk érni. A jelenlegi realitások között a rendőrség elé olyan középtávú célokat kell állítani az informatikai biztonság területén, amelyek egyrészt lehetővé teszik, hogy a testület a jelenlegi sok-sok gonddal küszködő „átmeneti állapotából” mielőbb kiemelkedjen, másrészt képes legyen az országnak az Európai Uniós tagságából adódó feladatok ellátására.

The strategy is a structurally special dual characterised aim-hierarchy – accordingly to the aims, stated in the Regional Strategy of the Hungarian Republic – and each aim can be conceptualized as an implement to reach another, higher aim. It can be perceived in the form of a specific aim-tool pyramid, in which the aim character strengthens into the direction of the top of the pyramid, and the tool character into the direction of the base of the pyramid. Its’ most important elements are the strategic aims, which summarize the most significant intentions of the police - in reference to the future, as well as the action-sectors, which are well-outlined segments of the realization of the strategic aims, and which conclude logically coherent tasks and task-packages – influencing the realization of concrete aims. Reflecting the above mentioned – the basic information technological security strategy for the police must formulate those future status-parameters, what we consider to be the most relevant ones and the ones we want to achieve in a long-term plan. On the base of the present reality those medium-term aims must be encountered with the police on the field of the information technological security, which can create the possibility for the police to emerge from the present-temporary state of many-many problems, and on the other hand, to make it to be able to fulfil the special tasks of the country – given by the member status of the European Union.

Kulcsszavak: *nagyobb biztonság, minőségi rendőri munka, stabil működési feltételrendszer, rendszerek megbízható üzemeltetése ~ higher security, qualitative police work, stabile working condition-system, responsible operation of the systems.*

BEVEZETÉS

Az Informatikai Biztonsági Stratégia elkészítésének célja, a rendőrségének Testületi Stratégiájában kitűzött célok eléréséhez az informatika eszközrendszerének mind hatékonyabb mozgósítása, olyan értékálló beruházások és fejlesztések eredményeként, melyek használatával javul a rendőrség reagáló képessége, növekszik a bűnelkövetők kockázatviselési kényszere, javul az állampolgárok valós biztonságérzete.

A stratégia kialakítása során figyelembe kell venni a jogszabályokban meghatározott követelményeket, a vonatkozó szabványokat és ajánlásokat, továbbá az információtechnológia fejlődéséből fakadó szempontokat.

A rendőrség informatikai stratégiájának szorosan kell kapcsolódnia a Belügyminisztérium informatikai feladataihoz, a szakirányítás eszközéül szolgáló informatikai stratégiájához. Álláspontom szerint, mindkét stratégia az informatika kiszolgáló jellegének hangsúlyozásán keresztül kíván eljutni kitűzött céljaihoz oly módon, hogy a hangsúlyt egyértelműen a szakmai (nem informatikai) vezetés által megfogalmazott feladatok kielégítésére helyezi.

A belügyminisztériumi informatikai stratégiájában megfogalmazottakat figyelembe véve az alábbi célterületeket vizsgáltam meg hogy meghatározzam a rendőrség informatikai biztonsági stratégiájának alapelveit:

- Rendvédelmi alkalmazások fejlesztése (határregisztrációs rendszer továbbfejlesztése, ujjnyomat nyilvántartó és azonosító rendszer továbbfejlesztése, egységes rendőrségi ügyfeldolgozó rendszer a Robotzsaru teljes körű kialakítása).
- Az informatikai szolgáltatási háttér rekonstrukciója (belügyi kezelésű alapnyilvántartások fejlesztése, egységes közgazdasági információs rendszer kialakítása, a választási információs rendszer, az ügyeleti rendszer továbbfejlesztése).
- Egységes hálózati infrastruktúra kialakítása (virtuális hálózatok kialakítása rendőrségi, határőrizeti, közigazgatási szolgáltatási feladatokhoz, egyenszilárdságú lokális hálózatok kialakítása, a távbeszélő szolgáltatások egységes, digitális szintre hozása, a ”112” hívószám használati feltételeinek végleges kialakítása, az EDR készenléti rádió-távközlési szolgáltatás bővítése, az országos funkcionális rejtjelezett kommunikáció megvalósítása).
- Közhitelességhez kapcsolódó alkalmazások kialakítása (Okmányirodák informatikai hátterének fejlesztése, a központi okmány-előállítás informatikai hátterének támogatása, az elektronikus átvitel hitelességének – biztonságának – megvalósítása).
- Közigazgatási szolgáltatások fejlesztése (Egységes címnyilvántartás kialakítása közigazgatási területi informatikai központokban, nyilvános lakossági információs rendszer korszerűsítése).

Vizsgálati körben, olyan új feladatok jelentek meg a rendőrség oldaláról (pl. a keleti határszakasz őrizetének és ellenőrzésének megerősítése, nemzeti adattár véglegesítése, a nyilvántartások adattartalmának, az adatvédelem elveinek, az elérhetőség technikai feltételeinek egységesítése), amelyek elengedhetetlenné teszik a határőrizet, a határforgalom-ellenőrzés, a menekült-, a migrációs és a bevándorlási politika és kapcsolatrendszerének, információs rendszereinek, technikai eszközeinek átértékelését. A fenti területek vizsgálatával olyan biztonsági követelményrendszert javaslok, melyet mind középtávú mind hosszú távú stratégiai célok elérésénél figyelembe kell vennünk.

A RENDŐRSÉG INFORMATIKAI STRATÉGIAI TERVE

Az informatikai stratégia kialakítása

Stratégián a célok, valamint a célok eléréséhez szükséges eszközök és módszerek együttesét értjük. A stratégia időbeli hatályát a rendőrség feladatrendszerének, a feladatrendszeren belül a súlypontokat meghatározó vezetői akaratnak, valamint az informatikai szakma eszközrendszerének változási sebessége is meghatározza.

A rendőrség informatikai stratégiájának szakmai célja a jelenlegi rendszerek megbízható üzemeltetése, az EU csatlakozás, a Schengeni rendszer követelményei szerinti fejlesztések előkészítése, a rendőrszakmai (vezetői, beosztotti) munkát támogató alkalmazások fejlesztésének kell, hogy legyen.

A stratégiánk kialakításához meg kell határoznunk, hogy

- hol vagyunk most - Helyzetértékelés,
- hová akarunk eljutni - Célkitűzés, elvárások,
- hogyan juthatunk oda - ennek megfelelő informatikai stratégia, feladatok meghatározása.

Ennek érdekében meg kell vizsgálnunk az *informatika kiszolgáló jellegét.* Az informatika nem cél, hanem eszköz. Az informatikai stratégiát a rendőrségnek szakmai célkitűzéseiből kell levezetnie. Érvényesíteni kell a környezeti feltételek rugalmas visszacsatolását, az interaktív szakmai tervezést, ezen belül:

- az alaptevékenységek szakmai prioritásait,
- az informatikai prioritásokat,
- a költségvetés-tervezési prioritásokat.

Az egységesség érvényesülésének elvét kell követni, hogy a fenti célkitűzések teljesüljenek.

A rendőrség a stratégiai terve kötelezően figyelembe veszi a BM által meghatározott szabványokat, ajánlásokat, egyéb előírásokat (melyek értelemszerűen tartalmazzák az Európai Unió, a NATO, valamint a nemzeti szabványokat), végrehajtja a szakmai célkitűzéseinek BM által való egyeztetését a közös elemek használása céljából más érintett szervezetek vonatkozásában. Harmonizációra törekszik a rendvédelmi és fegyveres szervekkel, illetve más államigazgatási, állami szervekkel egyaránt.

Ennek tükrében az informatikai stratégiának *egységesen kell kezelnie* az információrendszerek és alkalmazások, a számítástechnikai eszközök és a kommunikációs infrastruktúra korszerűsítésére irányuló fejlesztések tervezését és megvalósítását. Az egységességet (szabványosságot) meg kell valósítani mind az infrastrukturális, mind pedig az alkalmazásfejlesztéseknél.
Megvizsgálva a rendőrségre vonatkozó kormányhatározatokat, belügyi rendelkezéseket, azokat feldolgozva és a Közigazgatási Informatikai Bizottság (a továbbiakban: KIB), illetve a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság (a továbbiakban: MeH ITB) vonatkozó ajánlásait kell szem előtt tartani az informatika biztonsági stratégia megalkotásánál.

AZ INFORMATIKAI BIZTONSÁGI STRATÉGIA ALAPELVEINEK MEGHATÁROZÁSA

A követelményrendszer meghatározásánál feldolgoztam az ISO/IEC 27002:2005 szabványt, a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 10., 13. és 17. számú ajánlásait, továbbá a KIB 25. számú ajánlásából (Magyar Informatikai Biztonsági Ajánlás) a Magyar Informatikai Biztonsági Irányítási Követelményrendszer (MIBIK) részeit az Informatikai Biztonsági Irányítási Rendszert (IBIR), az Informatikai Biztonsági Irányítási Követelményeket (IBIK), az Informatikai Biztonsági Irányítás Vizsgálatát (IBIV), a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Sémát (MIBÉTS), továbbá az ezek alkalmazását támogató KIB 28. számú ajánlást, a KIB 19. számú ajánlását, alkalmazva a COBIT 4.1 és az ITIL V3 módszereket, követelményrendszerét [1-13]. Az alábbi alapelvek érvényesülését tartom fontosnak az informatikai biztonsági stratégia megalkotása során a rendőrségnél:

- *Bizalmasság:* biztosítani kell a rendőrség kezelésében és használatában lévő adatok, információk tekintetében mind a központi, mind a helyi feldolgozások, valamint az adat- és információcsere során, „hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról”[14]
- *Sértetlenség* folyamatosan biztosítani kell a rendőrség által kezelt, feldolgozott és közzétett adatokra mind a feldolgozás, mind pedig az adat- és információcsere során.
- *Rendelkezésre állás:* biztosítani kell a külső és belső adatkérések során, hogy az adatok az „arra jogosultak által a szükséges időben és időtartamra használható”

A három alapelvet tovább vizsgálva a stratégiai célkitűzések eléréséhez a további elvek szem előtt tartását javaslom a dokumentum elkészítéséhez:

A folyamatosság elve

Figyelembe kell venni az eddig megvalósult fejlesztéseket, szervesen kell építkezni azok eredményeire. Számításba kell venni a következő tervezési ciklusra maradó feladatokat, az informatika, a számítástechnika, a távadat-átvitel várható fejlődésének irányait, a hosszabb távra terjedő rendőri feladatokat.
A megvizsgált dokumentumok értelmezésiből elfogadtam, hogy *„Az informatika az információ természetével, a vele, kapcsolatos tevékenységekkel (gyűjtésével, ábrázolásával, továbbításával, tárolásával, feldolgozásával, védelmével, megsemmisítésével stb.), e tevékenységeket megvalósító és/vagy támogató rendszerekkel, továbbá a rendszerekkel, kapcsolatos tevékenységekkel (tervezés, fejlesztés, szervezés, üzemeltetés, kiértékelés, minőségbiztosítás) foglalkozó szakág.*[15]

A rendőrség tekintetében ezek alapján, értelmezésem szerint:
Az informatika rendőrség feladatrendszerébe illesztve olyan, az alapfeladatokat hatékonyan támogatni képes eszköz, mely a számítástechnika és a kommunikáció eszközrendszereinek felületi és működési integrálásával képes a rendőri alapfeladatok támogatásán túl, a civil közigazgatás és ezen keresztül az állampolgárok felé magas szintű szolgáltatást nyújtani.

Véleményem szerint, az informatika részének kell tekinteni a távközlést is, így a továbbiakban informatikai stratégián a rendőrség távközlési és számítástechnikai szolgáltatási egységeinek közös stratégiáját értem.

A Rendőrségnek a közbiztonsági helyzet javítására, a bűnözés visszaszorítására kidolgozott hároméves középtávú fejlesztési programja (1053/1997. (V.28.) Kormány határozat) [16] a szervezet erőforrásait minden területre kiterjedően mozgósítani kívánja, és a meglévő eszközrendszer optimális felhasználásával egy átfogó szolgáltatásfejlesztési folyamatot akar beindítani. Ezen szakmai célkitűzés értelmében az emberi, tárgyi és pénzügyi erőforrások sorába fel kell venni az információt is. Ahhoz, hogy az informatikát a Magyar Rendőrség erőforrásai közé fel tudjuk venni szükség, van a szervezet globális céljait és érdekeit érvényesíteni, és a részletekkel harmonizálni tudó vezetésre, irányításra, koordinációra, szervezeti és működési rendre.

Ennek gyakorlati megvalósításaként, a fejlesztési folyamat egyik közvetlenül vezérelhető és gyors eredményeket felmutató területe lehet a közterületi rendelkezésre állás hatékonyságának növelése. Ennek elérése érdekében szükségesnek tartanám a rendőrségi alapinfrastruktúra fejlesztését, különös tekintettel az informatika és a távközlés eredményeinek és lehetőségeinek felhasználására, mellyel növelhetővé válik az informatikai biztonság is.

A fokozatos fejlődés elve

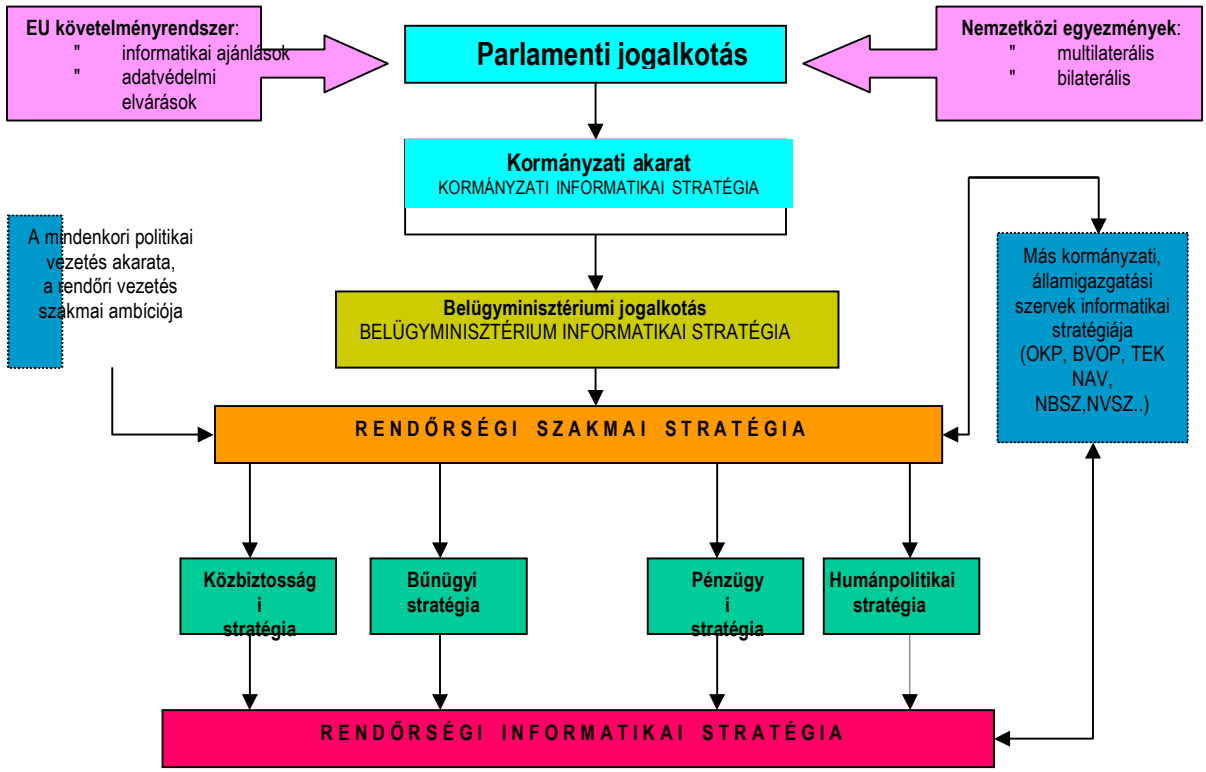
Az informatikai biztonsági stratégiának rövid helyzetértékelés alapján fel kell tudnia vázolni az informatikai alkalmazások lehetséges irányait, a rendőri munkát átfogóan támogató információrendszerek fejlesztésének és működtetésének alapelveit és rövidtávon kitűzhető céljait, valamint a megvalósítás lehetséges eszközrendszerét.
Véleményem szerint az informatikai biztonsági stratégia elfogadása és következetes megvalósítása jelentős előnyökkel jár, hisz a tervszerű rendőri munka nem nélkülözheti az informatika szolgáltatásait, másrészt az informatika mind újabb területeire hatol be a rendőri munkának, megváltoztatva és korszerűsítve az adott szakmai tevékenységet.
Jóllehet a korszerű informatikai megoldások iránti fogadókészség fokozatosan fejlődik, ma még számos területen hiányzik a vezetői elkötelezettség, a jogi keretek sem támogatják mindig ezen megoldások bevezetését. Az információ- és adatgazda szerepek, feladat-hatáskörök- és felelősségi viszonyok rendezetlenek, s ennek következtében a meglévő információrendszerek működési hatékonysága rendkívül alacsony.

A fokozatosság elvének teljesülését vizsgálva azt tapasztaltam, hogy informatikai rendszereknek a rendőrségen belül is kialakult egy jellegzetes rétegszerkezete, amelynek tipikus szintjei:

- Az univerzálisan használható, infrastruktúra jellegű hardver és alapszoftverek.
- Az erre épülő feladat-specifikus alkalmazói szoftverek.
- A szervezeti feltételeket, a szervezetbe való illeszkedést biztosító orgver, ami szabályzatokban, ügyrendekben, munkaköri leírásokban jelenik meg.
- A rendszerek teljes életciklusára kiterjedő szervezési feladatokat ellátó informatikai menedzsment.

Az állandó helyzetvizsgálat elve

Az informatika szerepe a világ minden nagy szervezeténél így a rendőrségnél is, hogy hatékonyan biztosítsa a szervezetszerű feladatok kiszolgálását a koncepcionálisan kitűzött szervezeti célok elérését. Az informatika tevékenység rendszerének helye és szerepe a rendőri tevékenységek rendszerében mindig változott.



Ahhoz, hogy tényszerű megállapításokat tegyünk, két irányt kell megvizsgálnunk a helyzetvizsgálat során: a kialakult informatikai helyzetet (Hol vagyunk most?) és az általános informatikai célkitűzéseket (Hova akarunk eljutni!)

Az első irány szerint, a rendőrség első önálló informatikai koncepciója 1991 végén, 1992 elején alakult ki. A koncepció lényegét röviden összefoglalva " 3-5 év alatt létre kell hozni az európai szintű informatikát a magyar rendőrségnél". A koncepció felső szintű elfogadását követő munkálatok elsődlegesen általános –extenzív növekedés keretében megvalósuló - modernizációs programot céloztak meg, kevésbé kötődtek konkrét rendőri szolgálati stratégiához. Ezt a koncepciót követték a többi, 5 évenként megújuló stratégia tervezetek is.

A második irány vizsgálatakor a megvalósítandó informatikai stratégia célja, a bűnügyi és közbiztonsági események jellegéből fakadóan, globális – az egész ország területére, bizonyos tekintetben az országhatárokon túlra is kiterjedő – rendőri szakmai munka támogatását célzó, a területileg és szervezetileg elszigetelt informatikai rendszerek közötti kapcsolat megteremtése, azaz egységes, országos rendőrségi információs rendszer kiépítése. A rendszer célja, hogy biztosítsa a rendőrségi alapfeladatok magasabb színvonalú ellátásához szükséges információk gyors és biztonságos áramlását, infrastruktúrát képezzen a szakmai munkát

támogató, valamint a rendőrség egészének működését biztosító globális és lokális számítástechnikai eszközök, rendszerek, alkalmazások futtatására.

Összefoglalva a két irányt: *A rendőrségi informatikai stratégia a meglévő informatikai és távadat-átviteli hálózati alapokra, a meglévő számítástechnikai eszközök és humán szakmai bázis felhasználásával egy – a rendőri alapfeladatokat támogató - szolgáltatási információs hálózat alapjait teremti meg.*

A biztonságra törekvés elve

Az informatikai biztonsági stratégia megtervezése során törekedni kell a biztonság megteremtése érdekében a további elvek érvényesítésére:

- Törvényesség garantálása.
- Hitelesség garantálása.
- Azonosítással hitelesítés.
- Elszámoltathatóság kialakítása.
- Hozzáférés-szabályozás.
- Jogosultság kiosztás és annak ellenőrzése.
- Auditálhatóság logikai védelmi funkcióinak megteremtése.
- Bizonyítékok rendszerének és folyamatának kialakítása.
- A hibákat elsősorban nem kijavítani, hanem megelőzni kell.

A rendőrség informatikai biztonságának megteremtése érdekében szabályozott formában, a stratégiában az alábbiakról kell gondoskodni:

- Az informatikai biztonság részletes követelményeinek rögzítése az informatikai biztonság dokumentációs rendszerben.
- Az informatikai biztonsággal kapcsolatos szervezeti és hatásköri kérdések, valamint a rendőrségen belüli és az azon kívüli adatkapcsolatok szabályozása.
- A rendőrség adat és információs vagyonának védelmét szolgáló minősítési és biztonság osztályba sorolási eljárás kialakítása, valamint annak ellenőrzési módja.
- A személyekhez és szerepkörökhöz kapcsolódó biztonság követelmények, az oktatási és képzési tervek, valamint biztonság események és meghibásodások esetén szükséges eljárások kialakítása.
- Az informatikai biztonsághoz kapcsolódóan az informatikai rendszerek fizikai és környezeti biztonságának kialakítása.
- Az alkalmazott üzemeltetési és kommunikációs eljárások informatikai biztonság követelményrendszerének meghatározása.
- Az informatikai eszközökhöz, adatokhoz és informatikai szolgáltatásokhoz történő hozzáférés szabályainak kialakítása és alkalmazása.
- Az informatikai rendszerfejlesztési és karbantartási eljárások létrehozása.
- Az informatikai infrastruktúra folyamatos működésének biztosítását szolgáló eljárások kialakítása.
- Az informatikai infrastruktúra, eljárások és szolgáltatások jogszabály megfelelőségét biztosító szabályozás kialakítása.
- A védelmi célkitűzések és informatikai biztonság követelmények teljesítése érdekében biztosítani kell a kellően költséghatékony, kockázatokkal arányos védelmi intézkedések és ellenőrzések – a mindenkori rendelkezésre álló erőforrásoknak megfelelő – alkalmazását.

- Az rendőrség informatikai biztonsági stratégiája, a már megfogalmazott informatikai biztonság filozófiára-politikájára kell épülnie, és megfelelő alapot kell teremtenie az informatikai biztonság célkitűzések meghatározásához.
- *Az informatikai biztonsági stratégiának minden lehetséges esetben a proaktív, azaz megelőzésre törekvő magatartást kell előnyben részesítenie a reaktív, azaz követő magatartással szemben.*
- Az informatikai biztonsági stratégiának az informatikai biztonsággal összefüggő szabályoknak, intézkedéseknek egységes értelmezését kell elősegítenie.

Az informatikai szervezetek irányítása

Az elmúlt időszakban fokozatosan kialakult egy informatikai szakszolgálat alapja, mely még nem kellően szabályozott, a munkamegosztás nincs megfelelően elhatárolva. Jórészt emiatt, a rendőrségi informatikai menedzsment számára az informatikai terület nehezen áttekinthető és kezelhető. Véleményem szerint *az eredményes informatikai tevékenység egyik alapfeltétele az informatikai szakszolgálat hivatalos létrehozása, a rendőrségi struktúrához illeszkedő tagolása, a hatáskörök és döntési folyamatok szabályozása.*

A központi, területi informatikai rendszerek megfelelő működtetéséhez megfelelő hozzáértésű rendszergazdákat kell biztosítani. Szakirányításukra többféle modell is elképzelhető, mivel mind az alkalmazó szervezet működési igényeinek, mind az informatikai szakma elvárásainak eleget kell, hogy tegyenek. Ennek tükrében két modellt választottam ki.

Az egyik modell a *központi szervezettől elvárható feladatok* körébe sorolom a rendőrség szakmai stratégiájának kidolgozásában való részvétel, majd ennek alapján az informatikai stratégia kidolgozása, éves tervekre történő lebontása, végrehajtása, karbantartása. A másik modell *az informatikai stratégiából fakadó szabványosítási feladatok ellátása* (eszközellátási szabványok, adatbázis szabványok, informatikai fejlesztési, üzemviteli, ellátási normatívák, intézkedések, utasítások kidolgozása).
Részleteiben az informatikai stratégiából fakadó rendszerfejlesztési feladatok ellátását az alábbiakban fejtem ki:

- Az informatikai stratégia megvalósítását biztosító gazdálkodási feladatok ellátása (költségvetés tervezés, költségvetéssel történő gazdálkodás, előirányzat felhasználás figyelés, kötelezettség nyilvántartás, köz- és egyéb beszerzések, szerződés nyilvántartás, eszköznyilvántartás, raktározás, stb.).
- Az informatikai stratégia eredményeként megjelenő üzemeltetési feladatok ellátása (országos rendszerek üzemeltetése, az amortizációs tevékenység ellátása, központi adatbázisokhoz való hozzáférés biztosítása, adattárakból történő szolgáltatás biztosítása, országos szerviztevékenység részleges ellátása).

Fejlesztés, koordináció, felügyelet szem előtt tartása

Az informatika stratégia megalkotásánál az informatikai fejlesztések területén a szolgálati ágak által megfogalmazott igények, és az ezek támogatására irányuló feladatok az elsődlegesek. Ezeknek az elvárásoknak való megfelelés érdekében az informatikusi szakgárdán belül ki kell alakítani az egyes szolgálati ágaknak megfelelően a szakreferensi feladatköröket, amelyek „kettős irányítással”, de az informatikai szervezeten belül látják el feladataikat. Biztosítani kell olyan informatikai képzettséggel, gyakorlattal rendelkező

szakembereket, akik szakterületek igényeit össze tudják hangolni az informatikai lehetőségekkel és a szakszolgálattal.

A biztonsági szempontokat figyelembe véve a fejlesztéseknél az előkészítő, a koordinációs feladatokra, a követelmények megfogalmazására, a késztermék átvételére erőforrást kell biztosítani. A fejlesztéseket professzionális szolgáltatást nyújtani tudó szervezetekkel kell elvégeztetni. A megfelelő színvonal gazdaságos biztosíthatóságához elsősorban a szolgáltatásvásárlást kell előnyben részesíteni, de erre specializálódott szolgáltató szervezetek kialakítása is alkalmazásra kerülhet. Ki kell alakítani az informatikai szakirányítást megalapozó modelleket, minőségbiztosítási elveket, szabályokat és ajánlásokat.

Az informatikai biztonsági stratégiai kérdésének tartom a fejlesztések során, hogy érvényesíteni kell az egységes rendszertechnika elvét. Létre kell hozni a központi adatszabványokat. A központi rendszerek vonatkozásában könnyen menedzselhető, áttekinthető jogosultsági rendszert kell kialakítani.

ÖSSZEGZÉS

Az Informatikai Biztonsági Stratégia elkészítésének célját meghatározva, a rendőrségének Testületi Stratégiájában kitűzött célok eléréséhez az informatika eszközrendszerének mind hatékonyabb mozgósítása, olyan értékálló beruházások és fejlesztések eredményeként, melyek használatával javul a rendőrség reagáló képessége, növekszik a bűnelkövetők kockázatviselési kényszere, javul az állampolgárok valós biztonságérzete.

A rendőrség informatikai stratégiájának szakmai célját a jelenlegi rendszerek megbízható üzemeltetése, az EU csatlakozás, a Schengeni rendszer követelményei szerinti fejlesztések előkészítése, a rendőrszakmai (vezetői, beosztotti) munkát támogató alkalmazások fejlesztésében állapítottam meg.
Figyelembe vettem a vizsgálat során a bizalmasság, sértetlenség, rendelkezésre állás alapelveit. Meghatároztam, hogy az informatika rendőrség feladatrendszerébe illesztve olyan, az alapfeladatokat hatékonyan támogatni képes eszköz, mely a számítástechnika és a kommunikáció eszközrendszereinek felületi és működési integrálásával képes a rendőri alapfeladatok támogatásán túl, a civil közigazgatás és ezen keresztül az állampolgárok felé magas szintű szolgáltatást nyújtani.

Rendszerbe szettem a rendőrség informatikai biztonsági stratégiájának megalkotása során alkalmazandó alapelvek sorát mely szerint:

- a folyamatosság elve:
- a fokozatos fejlődés elve
- Az informatikai biztonsági stratégiának rövid helyzetértékelés alapján fel kell tudnia vázolni az informatikai alkalmazások lehetséges irányait, a rendőri munkát átfogóan támogató információrendszerek fejlesztésének és működtetésének alapelveit és rövidtávon kitűzhető céljait, valamint a megvalósítás lehetséges eszközrendszerét.
- az állandó helyzet vizsgálat elve
- meghatároztam a rendőrségi informatikai helyét a rendőrségen belül és a kormányzaton belül
- Az iránymutatás szükségessége keretében a rendőrségi informatikai stratégia a meglévő informatikai és távadat-átviteli hálózati alapokra, a meglévő

számítástechnikai eszközök és humán szakmai bázis felhasználásával egy – a rendőri alapfeladatokat támogató - szolgáltatási információs hálózat alapjait teremti meg.

- a biztonságra törekvés elveként Az informatikai biztonsági stratégiának minden lehetséges esetben a proaktív, azaz megelőzésre törekvő magatartást kell előnyben részesítenie a reaktív, azaz követő magatartással szemben.
- az informatikai szervezetek irányítása szerint az eredményes informatikai tevékenység egyik alapfeltétele az informatikai szakszolgálat hivatalos létrehozása, a rendőrségi struktúrához illeszkedő tagolása, a hatáskörök és döntési folyamatok szabályozása.
- Fejlesztés, koordináció, felügyelet szem előtt tartása.

Összefoglalóan elmondható, hogy a rendőrség informatikai biztonsági stratégiája azon jövőbeni állapotjellemzőket kell, hogy fogalmazza meg, amelyeket a legfontosabbnak tartunk és hosszabb távon elkívánunk érni.

FELHASZNÁLT IRODALOM

[1] ISO/IEC 27002:2005 szabvány

[2] MEH ITB 10. számú ajánlás

[3] MEH ITB 13. számú ajánlás: Internet a Kormányzatban – Intranet, 1.0 verzió Budapest, 1997

[4] MEH ITB 17. számú ajánlás: Elektronikus adatcsere1.0 verzió Budapest, 1997

[5] KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Irányítási Követelményrendszer (MIBIK) 1.0

[6] KIB 25. számú ajánlása: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0

[7] KIB 25. számú ajánlása: az Informatikai Biztonsági Irányítási Követelmények (IBIK) 1.0

[8] KIB 25. számú ajánlása: Informatikai Biztonsági Irányítás Vizsgálata (IBIV) 1.0

[9] KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)

[10] KIB 28. számú ajánlása: E-Közigazgatási Keretrendszer 1.0

[11] KIB 19. számú ajánlása: A közigazgatás szervezetei által működtetett honlapok tartalmi és formai követelményeire, verzió: 3.0

[12] COBIT (Control Objectives for Information and related Technology) "Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések" verzió 4.1, IT Governance Institute, 2007.

[13] ITIL (IT Infrastructure Library) az informatikai szolgáltatásmenedzsment verzió: V3 2011.

[14] Muha Lajos: az informatikai biztonság egy lehetséges rendszertana, Bolyai Szemle XVII. évf. 4. szám, pp 137-156., 2008.

[15] Az Informatikai Tárcaközi Bizottság (ITB) 10.sz. ajánlásaként kiadott „ A központi államigazgatás informatikai stratégiája 1995-0997.”, INFORMATIKAI TÁRCZKÖZI BIZOTTSÁG Melléklet a kormányzati informatikai koordináció továbbfejlesztésére készített kormány-előterjesztés tervezetéhez , Budapest, 1995. http://www.itb.hu/dokumentumok/archivum/bg.html

[16] 1053/1997. (V.28.) Kormány határozat A Rendőrségnek a közbiztonsági helyzet javítására, a bűnözés visszaszorítására kidolgozott hároméves középtávú fejlesztési programja Magyar Közlöny 26.szám

HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Munk Sándor – Serege Gábor
munk.sandor@uni-nke.hu – serege.gabor@uni-nke.hu

A MAGYAR HONVÉDSÉG HÍRADÓ ÉS INFORMATIKAI HÁLÓZATÁNAK FOGALMA, ÉRTELMEZÉSE, ÉS A KAPCSOLÓDÓ HÁLÓZATFOGALMAK

Absztrakt

A Magyar Honvédség honvédelmi célú híradó-informatikai hálózatával kapcsolatban számos eltérő, közös értelmezési problémákat okozó elnevezéssel találkozhatunk. A publikáció célja kettős. Egyrészt a különböző szintű hatályos szabályzók, vonatkozó dokumentumok, illetve tudományos publikációk fogalmi rendszerének vizsgálatán keresztül feltárja a leggyakrabban használt elnevezéseket és eltéréseket, másrészt a kutatási eredmények alapján ajánlást fogalmaz meg.

By examining the labelling pattern of the communications network of Hungarian Defence Forces, there could be found several misnomer. This publication has two goals. One hand it opens up the most frequent naming schemas and deviations, and the other hand considering the results it gives nomination.

Kulcsszavak: *Magyar Honvédség, hálózat, fogalom ~ Hungarian Defence Forces, network, concept*

BEVEZETÉS

A Magyar Honvédség híradó, informatikai és információvédelmi szakterülete, valamint az ezen szakterület támogatását felhasználó vezetési, hadműveleti, stb. szakterületek szakmai és tudományos dokumentumaiban a polgári szakirodalomhoz hasonlóan számos különböző hálózatfogalommal találkozhatunk, amelyek többnyire konkrét meghatározás, értelmezés nélkül, esetleg különböző, egymással ütköző értelmezéssel kerülnek felhasználásra. Egységesen értelmezett hálózatfogalmak nélkül azonban nincs remény a konvergáló, integrálódó szakterületek összehangolt együttműködésére, egymást erősítő tevékenységére.

A fenti célok megvalósításának elősegítésére a következőkben összegezzük a MH híradó és informatikai hálózata fogalmának meghatározása során felhasznált fogalmi alapokat, értelmezéseket, a teljesség igénye nélkül röviden áttekintjük a Magyar Honvédségben felhasznált hálózatfogalmakat és kapcsolatrendszerüket[1], végül meghatározzuk a MH híradó és informatikai hálózatának javasolt fogalmát, értelmezését és határait.

HÁLÓZAT- ÉS RENDSZERFOGALMAK, ÉRTELMEZÉSÜK VIZSGÁLATÁNAK ALAPJAI

Jelen publikációban a hálózatfogalmak és értelmezésük vizsgálatának alapjai egy korábbi, az információs szolgáltatásokat nyújtó hálózatok kérdéseit tárgyaló publikációra[2] épülnek. Ezen publikáció alapfogalma a technikai hálózatok egyik – rendeltetése alapján elkülönített – alapvető típusa, az *információs szolgáltatásokat nyújtó [technikai] hálózat*, amelynek rendeltetése információs tevékenységek támogatása, megvalósítása. Ezen hálózatok elemei (csomópontjai) információs képességekkel rendelkező technikai eszközök (rendszerek), amelyek között információtovábbítást, információcserét biztosító valós fizikai, vagy absztrakt – más hálózatok szolgáltatásaira épülő – logikai kapcsolatok állnak fent. [1, 229. o.]

Az információs szolgáltatásokat nyújtó hálózatok közül először a konkrét információtovábbítási szolgáltatásokat megvalósító típusok – ezek között a különböző távközlő és műsorszóró hálózatok – jelentek meg. Ezt követték az információk, információs képességek megosztását biztosító számítógép-hálózatok. A technológiai fejlődés következtében mára előtérbe kerültek a több információs tevékenységet támogató, integrált információs szolgáltatásokat nyújtó hálózatok. A konvergencia és integráció következtében napjaink hálózatai már egyre kevésbé sorolhatóak be a szakterületi kategóriákba (távközlő hálózat, számítógép-hálózat, műsorszóró hálózat), vagy teljes joggal sorolhatóak be több kategóriába is. Az átfogó fogalom megnevezésére egyelőre nem alakult ki egységesen elfogadott kifejezés.

Vizsgálatunkhoz megkerülhetetlen az *információs szolgáltatásokat nyújtó rendszerek és hálózatok* fogalmainak értelmezése, azonosságuk, vagy különbözőségük, kapcsolatrendszerük és elhatárolásuk elemzése. A szakirodalomban – és a Magyar Honvédség esetében, mint azt a későbbiekben részletesebben be is mutatjuk – a két fogalom értelmezése, megkülönböztetése, a két kifejezés használata nem egyértelmű. Az információs szolgáltatásokat nyújtó hálózatok tartalmilag minden tekintetben megfelelnek a rendszerfogalom kritériumainak, így kellő önállóság esetén (speciális) rendszernek is tekinthetőek. Ugyanakkor a két kifejezés ugyanazon jelzővel számos esetben 'rész / egész', vagy 'szolgáltatást igénybe vevő / szolgáltatást nyújtó' viszonyra utal. A hálózatok és rendszerek viszonya alapvetően attól függ, hogy hol húzzuk meg a hálózat határait, mit tekintünk a hálózat részének és mit azon kívül álló összetevőnek. [1, 233. o.] Az elhatárolásnak kisebb a jelentősége a dedikált hálózattal rendelkező rendszerek esetében, azonban irányítási, felügyeleti szempontból lényeges szerepet játszik a szolgáltatói hálózatokra épülő önálló rendszereknél.

[1] Ez önmagában egy önálló kutatási feladatot jelenthet, ami túlnő a jelen publikáció keretein.
[2] Munk Sándor: Informatikai szolgáltatásokat nyújtó hálózatok alapjai. [1]

Egy *hálózat határai* több szempontból is vizsgálandóak. Ezek közé tartozik egyes hálózati összetevők hálózathoz tartozásának meghatározása, illetve a horizontálisan együttműködő és a vertikálisan szolgáltatásokat nyújtó hálózatokkal fennálló határok kijelölése. A határok az egyes összetevők esetében értelmezésünk szerint a rendeltetés, a nyújtott szolgáltatásokhoz történő hozzájárulás alapján határozhatóak meg. A hálózatok összetevőinek főbb típusait a hálózati szolgáltatások igénybevételét biztosító és a szolgáltatásokat nyújtó csomópontok (végpontok), valamint a hálózati információáramlást megvalósító, biztosító csomópontok (belső pontok), illetve a csomópontokat hálózatba kapcsoló összeköttetések képezik.

A hálózatok határainak meghúzása szempontjából a két nagy csoportot a felhasználók által közvetlenül igénybe vehető, végszolgáltatásokat nyújtó hálózatok és a más rendszerek (esetleg hálózatok) számára átviteli, hordozó szolgáltatásokat nyújtó hálózatok képezik. Ez utóbbiak csak az információtovábbítást biztosító csatolóelemeket (interfészeket), kapcsolóelemeket és átviteli vonalakat foglalják magukban, míg a végszolgáltatásokat nyújtó hálózatok részét képezik a szolgáltatások igénybevételét biztosító végberendezések, valamint a szolgáltatások nyújtásában részt vevő (kiszolgáló) eszközök, berendezések. [1, 235. o.] Elképzelhető olyan körülhatárolás is, amelyben egyes szolgáltatások végberendezései és kiszolgáló eszközei a hálózat részét képezik, míg más szolgáltatások esetében nem.

Az információs szolgáltatásokat nyújtó hálózatok megfelelnek a rendszer-kritériumoknak, így esetükben is értelmezhető az *alhálózat (alrendszer)* fogalma, illetve hálózatok, mint összetevők összekapcsolódhatnak egy nagyobb hálózatban (amelynek így alhálózatait képezik). A rendszerelméleti megközelítésnek megfelelően az alhálózat egy nagyobb hálózat olyan része (összetevője), amely önmagában is hálózatnak tekinthető. Csomópontjai és kapcsolatai közé az eredeti hálózat csomópontjainak és kapcsolatainak egy része tartozik. Összetett hálózat alatt pedig olyan hálózatot értünk, amelyen belül önálló alhálózatok különíthetőek el.

Egy hálózati eszköz-együttes önálló hálózatnak (alhálózatnak) a rendeltetés, a technológia, az irányítás/felügyelet, a biztonsági követelmények/megoldások, valamint a földrajzi elhelyezkedés alapján tekinthető. Elemi hálózatnak egy meghatározott rendeltetésű, valós fizikai kapcsolatokra épülő, egységes irányítás alatt álló hálózatot (erőforrás-rendszert) célszerű tekinteni. Ezen felül további kritérium lehet az alkalmazott technológiai megoldás (valamilyen szintű) azonossága is. [1, 236. o.]

A MAGYAR HONVÉDSÉG MEGHATÁROZÓ KÖRNYEZETE HÁLÓZAT-FOGALMAI

A Magyar Honvédség meghatározó környezete hálózat-fogalmai sorába a magyar kormányzati szabályozókban és az alapvető NATO dokumentumokban szereplő fogalmak sorolhatóak. A következőkben ezek közül a legfontosabbaknak ítélteket vesszük sorra.

A *kormányzati szabályozók* közül alapvető szerepet az elektronikus hírközlésről szóló törvény [2] és a kormányzati célú hálózatokról szóló kormányrendelet [3] játszik. A törvény tartalmazza a kormányzati célú hálózat fogalmát, amely "jogszabályban meghatározott közfeladatok ellátásához szükséges olyan elektronikus hírközlő hálózat …, amely nyilvános elektronikus hírközlő hálózattól fizikailag, vagy logikailag elkülönített". [2, 1. § (2)] Az elektronikus hírközlő hálózat "átviteli rendszerek és – ahol ez értelmezhető – a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások – beleértve a nem aktív hálózati elemeket is –, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálóza-

tokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára."[3] [2, 188. §, 19.] A kormányrendelet feljogosítja a Magyar Honvédséget (a honvédelmi minisztert) hogy kormányzati célú elkülönült – a kormányzati célú hírközlési szolgáltatótól független – hírközlő hálózatot működtessen, amelynek megnevezése 'a Magyar Honvédség honvédelmi célú híradó-informatikai hálózata'. [3, 2. mell.]

A NATO dokumentumok közül alapvető szerepet a *NATO fogalomjegyzék* [4] játszik, amelyben információs szolgáltatást nyújtó 'hálózat' fogalom nem szerepel, helyette a 'communication and information systems (CIS)', 'communication system (CS)', 'information system (IS)' és 'NATO consultation, command and control systems (NC3S)' fogalmak találhatóak. A kifejezések magyar fordítása nem egységes, a következőkben mi a szélesebb körben elfogadott – és megítélésünk szerint szakmailag megalapozott – terminológiát használjuk.

A fogalmak meghatározása a fogalomjegyzékben a következő:

- híradó rendszer: Eszközök, módszerek és eljárások, illetve működtető személyzet információtovábbítási funkciók megvalósítására létrehozott rendszere. Megjegyzések: 1. A híradó rendszer kommunikációt biztosít felhasználói között és magában foglalhat átviteli, kapcsoló és felhasználói rendszereket. 2. A híradó rendszer magában foglalhat az információtovábbítást támogató tároló, vagy feldolgozó funkciókat is. [4, 2-C-11. o.]
- informatikai rendszer: Eszközök, módszerek és eljárások, illetve működtető személyzet információfeldolgozási funkciók megvalósítására létrehozott rendszere. [4, 2-I-4. o.]
- híradó és informatikai rendszer: A híradó és az informatikai rendszerek gyűjtőfogalma. [4, 2-C-11. o.]
- NATO konzultációs, vezetési és irányítási rendszerek: Híradó és informatikai rendszerek, szenzorrendszerek és létesítmények, amelyek lehetővé teszik a NATO hatóságok és parancsnokságok konzultációs, vezetési és irányítási tevékenységét. [4, 2-N-1. o.]

A fenti fogalmakat a *NATO híradó és informatikai fogalomjegyzék* lényegében azonos tartalommal szerepelteti [5, 2-8, 2-9, 2-11, 2-17. o.], azzal a kiegészítéssel, hogy az informatikai rendszer meghatározása megjegyzésként tartalmazza a következőket: 1. Példák informatikai rendszerekre: vezetési és irányítási informatikai rendszer, igazgatási informatikai rendszer, irodaautomatizálási rendszer. 2. Egy informatikai rendszer a feldolgozási funkciók támogatására továbbíthat információkat, például egy informatikai rendszer részét képező számítógépeket összekapcsoló helyi hálózaton keresztül. [5, 2-17. o.] A fogalomjegyzékben ezek mellett megtalálható a távközlési hálózat és a számítógép-hálózat fogalma is a következő tartalommal:

- távközlési hálózat (telecommunication network): mindazon eszközök összessége, amelyek távközlési szolgáltatásokat biztosítanak különböző helyek között, ahol berendezés biztosítja a hozzáférést ezen szolgáltatásokhoz; [5, 2-36. o.]
- számítógép-hálózat (computer network): Egymással adatkommunikációs céllal összekapcsolt adatfeldolgozó csomópontok hálózata. [5, 2-10. o.]

Témánk szempontjából a *NATO doktrínák* közül kiemelt szerepet a 2011-ben megjelent szövetségi híradó és informatikai doktrína [6] játszik. A doktrína alapvető fogalma a híradó és informatikai rendszer. A NATO híradó és informatikai rendszerek jellemzője a 'föderatív' jelleg, a különböző technikai, eljárási és biztonsági jellemzőkkel rendelkező, egymástól füg-

[3]A törvényben szereplő meghatározás megegyezik egy vonatkozó európai uniós szabályozó fogalom-meghatározásával.

getlenül létrehozott és üzemeltetett összetevőkre épülő felépítés. Ehhez kapcsolódóan a rendszerek önállóan irányított, felügyelt és üzemeltetett tartományokra[4] tagolhatóak. [6, 1-10. o.]

A MAGYAR HONVÉDSÉG HÁLÓZAT- ÉS KAPCSOLÓDÓ FOGALMAI

A Magyar Honvédség hálózat- és kapcsolódó fogalmai a meghatározó biztonságpolitikai dokumentumokban, a doktrínákban, az intézkedésekben, valamint a szakmai, tudományos anyagokban találhatóak. A következőkben röviden az ezekben szereplő terminológiát és értelmezéseket tekintjük át.

A *Magyar Köztársaság alapvető biztonságpolitikai dokumentumai* szintjükből következően részletesebben nem foglalkozhatnak vizsgálatunk tárgyát képező hálózatokkal, de a nemzeti biztonsági stratégia [7] az információs társadalom kihívásaival foglalkozó pontban fogalmazza meg a számítógépes hálózatok és rendszerek sebezhetőségének, túlterhelhetőségének kockázatát, a nemzeti katonai stratégia [8] pedig a képességalapú haderőfejlesztés legfontosabb feladatai között elsőként említi a tábori híradó és informatikai rendszerek rendszerszemléletű fejlesztését.

A magyar katonai doktrínák közül az *összhaderőnemi doktrína* fogalomrendszerét vizsgáljuk meg. A doktrína 1. kiadásának témánk szempontjából alapfogalma a 'híradó és informatikai rendszer', "a különböző vezetési szintek tevékenységéhez szükséges, rugalmasan változtatható, egységes elvek, módszerek és tervek alapján létrehozott; feladat, hely és idő szerint koordinált híradó és informatikai eszközök, eljárások, valamint az információs tevékenységeket végrehajtó szakállomány összessége". [9, 1101. pont] és ennek béke (állandó), illetve tábori összetevői. Emellett megjelenik a 'híradó és informatikai hálózatok' kifejezés is [9, 1114. pont], de meghatározás nélkül. A 2007-ben megjelent 2. kiadásban [10] lényegében ugyanez szerepel, de a dokumentum más részeiben megjelennek a 'számítógép hálózat' és 'informatikai hálózat' kifejezések is.

A napjainkban is hatályos *intézkedések* közül érdemes kiemelni a Magyar Honvédség állandó jellegű távközlő hálózatának békeidejű üzemeltetési és felügyeleti rendjéről szóló 47/2003. Honvéd Vezérkar Főnök intézkedést és az ugyan ezen évben a 61/2003. számú Vezetési Csoportfőnökség által kiadott szakintézkedést a MH állandó jellegű távközlő hálózatának békeidejű üzemeltetési és felügyeleti rendjének részletes szabályairól. Az intézkedés alapján az MH zártcélú hálózata magába foglalja az állandó jellegű távközlő hálózatot és a tábori hírrendszert is. A II. Értelmező rendelkezések-című fejezet egyértelműen meghatározza ezen 'híradó' hálózat összetevőit és elemeit, azonban egyetlen pontjában sem tesz említést a működő informatikai alhálózatról. A szakintézkedés ezzel szemben már nem csak a távközlési, hanem a távközlési és informatikai célú szolgáltatások biztosítását szabályozza. Logikailag ebből az a következtetés vonható le, hogy a Magyar Honvédségben működik egy az intézkedés által részletesen leírt távközlési (tisztán híradó) hálózat, amely távközlési szolgáltatásokat nyújt, és mellette üzemel egy olyan informatikai szolgáltatásokat biztosító hálózat, amelynek pontos meghatározása a mai napig várat magára.

A szakmai és tudományos dokumentumok leggyakrabban alkalmazott hálózatfogalmai vizsgálatához a Zrínyi Miklós Nemzetvédelmi Egyetemen készített híradó, informatikai és információvédelmi vonatkozású doktori disszertációkat, illetve a Hadmérnök online tudományos folyóirat archívumában fellelhető publikációkat vettük alapul. A vizsgált művek körének célzott behatárolását egyrészt a Magyar Honvédséghez fűződő szoros kapcsolatuk, másrészt a polgári élettől eltérő speciális környezet indokolta.

Az áttekintett 22 *híradó és informatikai témájú doktori értekezés* jelentős részében igényként jelenik meg a híradó és informatikai rendszerrel kapcsolatos általános fogalmak megha-

[4] Például felhasználói és hálózati, illetve NATO, műveleti és nemzeti tartományok.

tározására való törekvés. Megállapítható, hogy az elterjedt szakmai terminológiák egyöntetű, közös értelmezésének hiánya nem kérdéses. Az eltérő jelentésű fogalmak egymást helyettesítő használata értelmezési problémához vezethet. A definíciók újbóli lefektetésének okát a szakmai körökben általánosan használt, azonban sokszor eltérő tartalmú értelmezésben kell keresni. Ez tükröződik az alábbi idézetekben is, ahol a szerzők saját fogalmi iránymutatással vezetik be doktori értekezésüket, elkerülve ezzel a fogalmak „nem megfelelő" használatának vádját:

„Már a bevezetésben szükségesnek tartom értelmezni a híradás fogalmát…" - írja Magyar Sándor. [11, 5. o.]

„Elöljáróban célszerű néhány olyan fogalmat tisztázni, amelyek az értekezés célkitűzéseinek teljesítését, valamint az egységes értelmezését megkönnyítik."–. [12, 8. o.]

„…egyre szélesebb körben alkalmazott kifejezések keveredése a kommunikációs rendszer értelmezése során félreértésekhez vezethet."[12, 11. o.] - írja doktori értekezésében Pándi Erik

A fogalmi keveredés oka több tényezőre vezethető vissza:

- Egyrészt kiemelnénk a vonatkozó aktuális állapotokat tükröző szabályzók hiányát, amely problémára már 2003-ban felhívta figyelmünket Szenes Zoltán Vezérkar Főnök is: „"A szervezeti változások, a technikai fejlesztések miatt a már kidolgozott dokumentumok is több tekintetben elavultak. A minisztérium és parancsnokságok gyakori átszervezése miatt a doktrínaíró csoportok nem tudtak stabilizálódni, fordításra, kiadásra nem volt elég forrás." [13]
- Másrészt nem szabad figyelmen kívül hagyni olyan estet sem, amikor maga a szerző is tisztában van a nem pontos fogalmak használatának tényével, azonban az eltérő (régi és új) elnevezések felcserélhető használatának gyakorlatát a történeti hűség kedvéért mégis alkalmazza. [14]
- Harmadrészt egyszerűen szinonim, azonos jelentésű fogalmakként használják az egyébként eltérő tartalmú szakszavakat.

Megvizsgálva a leggyakrabban előforduló, egymás szinonim párjaként megjelenő fogalmakat, egyértelműen kitűnik a hírrendszer és a konvergencia jelenlétét tükröző híradó és informatikai rendszer fogalmának egyenértékű használata.

A *Hadmérnök publikációk* vizsgálata során az első évfolyam 2006. júniusi számától a hatodik évfolyam 2011. szeptemberi számáig tekintettük át az összes védelmi elektronika, informatika, kommunikáció témában, megjelent magyar nyelvű publikációt, mindösszesen 131 darabot.[5]. Kitűzött célunk volt felderíteni a „hálózat" és „rendszer" szavak előfordulási változatait és vizsgálni, hogy a szerző meghatározza-e az általa használt fogalmak jelentését olyan művekben, ahol a Magyar Honvédség honvédelmi célú híradó és informatikai hálózatával kapcsolatos gondolatokat fogalmaz meg, vagy épp „csak" bevett gyakorlatként használja azokat, és az olvasóra bízza a „megfelelő" értelmezést. A vizsgálat számszerű összefoglalását az 1. táblázat szemlélteti, míg a használt elnevezéseket a 2. táblázat tartalmazza.

Hálózat		**Rendszer**			
def.	**nem def.**	**def.**	**nem def**	**Év**	**Darabszám**
	3		5	2006	10
	2	1	5	2007	17
	5		3	2008	23
	2	2	5	2009	22
	1		2	2010	46
	0		0	2011	13

1. táblázat. Hálózat és rendszer szavak előfordulása a vizsgált publikációkban

[5] A vizsgált halmazba nem tartoztak bele a szerzők saját művei.

HÁLÓZAT	RENDSZER
helyi	informatikai
magán	katonai kommunikációs
állandó	katonai informatikai
dedikált	számítógép
informatikai	információs
adatátviteli	védelmi célú informatikai
számítógépes	infokommunikációs
zártcélú	számítógépes és hálózati
számítógép és számítógépes	informatikai rendszerek és hálózatok
infokommunikációs	

2. táblázat. Hálózat és rendszer jelzők

Az 1. táblázat számadataiból kitűnik, hogy a cikkek 21,37 százalékban használják a vizsgált szavakat, szóösszetételeket a Magyar Honvédség vonatkozásában.

Három esetben találtunk olyan művet, amelyben a szerző törekedett a fogalmak beazonosítására:

- Kerti András a MH infokommunikációs rendszere elnevezést használja és annak meghatározását a tartalmi elemeinek (kiépítendő összeköttetések) felsorolásával teszi. [15]
- Jobbágy Szabolcs publikációjában a fentebb említett intézkedésben és szakintézkedésben fellelt kettősség mutatkozik meg. Néhol hagyományos értelemben használja a hírrendszer fogalmát[6], más esetekben pedig az informatikai hálózatokkal kibővítetten: „A békeidejű híradó és informatikai rendszerek alapját a Magyar Honvédség állandó telepítésű, úgynevezett stacioner híradó és informatikai hálózatok alkotják,…” [16]
- Töreki Ákos a stacioner kommunikációs rendszer megfogalmazást használja, aminek a meghatározásához egyet ért Fekete Károly doktori értekezésében leírt definícióval.

A publikációkban használt fogalmak gyakorisága alapján a szerzők a híradó és informatikai-, valamint az infokommunikációs hálózat, illetve rendszer kifejezéseket alkalmazták. A hálózat és rendszer fogalmakat egymás szinonimájaként, vagy épp halmaz részhalmaz kapcsolatként tüntették fel.

ÖSSZEGZÉS

A fentiek alapján a Magyar Honvédség híradó és informatikai hálózata javaslatunk szerint a Magyar Honvédség[7] irányítása, felügyelete alatt álló, információtovábbítási, információcsere szolgáltatásokat nyújtó technikai hálózatok összessége. A fenti meghatározásnak megfelelően a MH híradó és informatikai hálózata a MH híradó és informatikai rendszerének része, infrastrukturális összetevője. Szolgáltatásainak köre kiterjed a hagyományos távközlési (vezetékes és mobil távbeszélő, géptávíró stb.), az informatikai rendszereket, eszközöket összekapcsoló adatátviteli, valamint a különböző speciális rendeltetésű (pld. műsorszóró/elosztó, térfigyelő, érzékelő és más) hálózatok átviteli szolgáltatásaira.

A Magyar Honvédség híradó és informatikai hálózata részét képezik: a hálózathoz történő hozzáférést biztosító csatolóeszközök, berendezések, a hálózati kapcsolóelemek, a csomópontok közötti valós fizikai, vagy absztrakt logikai összeköttetések; a hálózat felügyeletének, üzemeltetésének rendszerei és eszközei, valamint az üzemeltető személyzet. Nem tartoznak a

[6] Hírrendszer: híradó erők és eszközök szervezeti, rendszertechnikai egysége…

[7] Konkrétabban a különböző szabályozókban meghatározott honvédelmi szervezetek, személyek.

hálózathoz az önállóan is működőképes, információs szolgáltatásokat igénybe vevő, vagy nyújtó rendszerek, eszközök.

A Magyar Honvédség híradó és informatikai hálózata az érintett területekkel, szervezetekkel történő együttműködés támogatására – közvetlenül (egyenrangú módon), vagy közvetve (egy gerinchálózaton keresztül) – kapcsolódik magyar kormányzati, rendészeti, katasztrófavédelmi, nemzetbiztonsági, stb. hálózatokhoz, valamint NATO és EU állandó és műveleti hálózatokhoz. A Magyar Honvédség híradó és informatikai hálózata saját működésének megvalósítása, illetve az előzőekben felsorolt együttműködési feladatok érdekében felhasznál(hat)ja a magyar kormányzat, a NATO, az EU és polgári szolgáltatók hálózatainak szolgáltatásait.

Felhasznált irodalom

[1] Munk Sándor: Információs szolgáltatásokat nyújtó hálózatok alapjai. – *Hadmérnök*, 2011 (VI.)/2. (227-243. o.) http://www.hadmernok.hu/2011_2_munk.pdf, 2012-01-15

[2] *2003. évi C. törvény az elektronikus hírközlésről.*

[3] *346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról.*

[4] *AAP-6(2010), NATO Glossary of Terms and Definitions (English and French).* – NATO Standardization Agency, 2010.03.22.

[5] *AAP-31(A), NATO Glossary of Communication and Information Systems Terms and Definitions.* – NATO Standardization Agency. 2003.05.15.

[6] *AJP-6, Allied Joint Doctrine for Communication and Information Systems.* – NATO Standardization Agency, 2011.04.06.

[7] *2073/2004. (III. 31.) Korm. h. a Magyar Köztársaság Nemzeti Biztonsági Stratégiájáról.*

[8] *1009/2009. (I. 30.) Korm. h. a Magyar Köztársaság Nemzeti Katonai Stratégiájáról.*

[9] *Magyar Honvédség Összhaderőnemi Doktrína.* – HM HVK Hadműveleti Csoportfőnökség, 2002.

[10] *Magyar Honvédség Összhaderőnemi Doktrína. 2. kiadás.* – Honvédelmi Minisztérium, 2007.

[11] Magyar Sándor: *Katonai kommunikációs igények, lehetőségek a békefenntartás vezetésének támogatásában. Doktori (PhD) értekezés.* - ZMNE, 2008

[12] Pándi Erik: *A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai-, és közigazgatási kommunikációs rendszerek megszervezésre és irányítására. Doktori (PhD) értekezés.* – ZMNE, 2005

[13] Szenes Zoltán: Magyar Honvédség a NATO-ban. Mit várhatunk Rigától? – *Hadtudomány*, 2006 (XVI.)/4. http://www.zmne.hu/kulso/mhtt/hadtudomany/2006/4/2006_4_6.html, 2012-01-15

[14] Fekete Károly: *A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei. Doktori (PhD) értekezés.* – ZMNE, 2003

[15] Kerti András: Átviteli út biztonság. – *Hadmérnök*, 2007 (II.)/4. (60-65. o.) http://www.hadmernok.hu/archivum/2007/4/2007_4_kerti.pdf, 2012-01-15

[16] Jobbágy Szabolcs: Híradás, hírrendszer, vezetés –irányítási rendszer fogalmi kitekintő. - *Hadmérnök*, 2010 (V.)/1. (247-256. o.)
http://www.hadmernok.hu/2010_1_jobbagy.pdf, 2012-01-15

[17] Töreki Ákos: A Magyar Honvédség stacioner kommunikációs rendszerének vizsgálata. – *Hadmérnök,* 2010 (V.)/1. (325-330. o.)
http://www.hadmernok.hu/2010_1_toreki.pdf, 2012-01-15