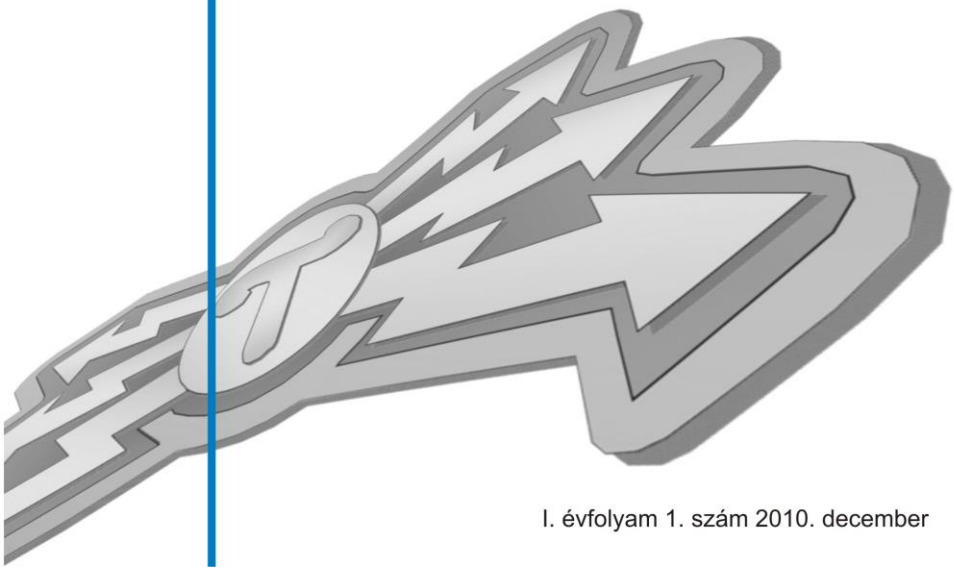
HÍRVILLÁM

A Zrínyi Miklós Nemzetvédelmi Egyetem
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL BADGE

Professional journal of Signal Department
at the Zrínyi Miklós National Defence University



I. évfolyam 1. szám 2010. december

A Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék tudományos időszaki kiadványa

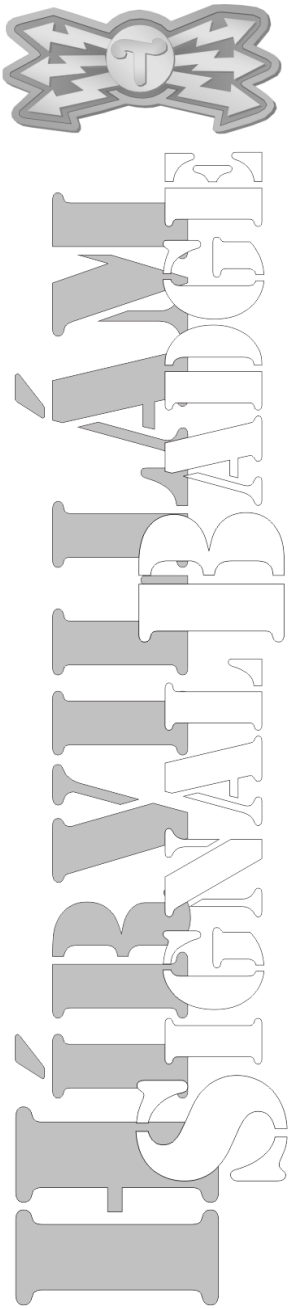
Professional journal of the Signal Department at the Zrínyi Miklós National Defence University

Megjelenik évente két alkalommal

Published twice a year

2010. december


ZMNE
BOLYAI



Felelős kiadó/Editor in Chief:

Dr. Rajnai Zoltán mk. ezredes, egyetemi tanár

Szerkesztőbizottság/Editorial Board:
Elnök/Chairman of the Board:

Dr. Fekete Károly mk. alezredes

Elnökhelyettes/Depute Chairman:

Töreki Ákos főhadnagy

Tagok/Members:

Czirok Ferenc r. ezredes
Dr. Farkas Tibor főhadnagy
Halmai Ottó mk. dandártábornok
Horváth Ferenc dandártábornok
Dr. Hóka Miklós nyá. mk. alezredes
Dr. Horváth Zoltán okl. mk. alezredes
Jobbágy Szabolcs főhadnagy
Dr. Kassai Károly mk. ezredes
Dr. Kerti András mk. alezredes
Dr. Lindner Miklós nyá. altábornagy
Mógor Tamásné százados
Dr. Osváth Zoltán nyá. mk. alezredes
Dr. Pándi Erik r. ezredes
Dr. Révész Gyula mk. ezredes
Dr. Sándor Miklós nyá. ezredes
Dr. Som Ferenc nyá. okl. mk. alezredes
Dr. Szöllősi Sándor nyá. okl. mk. őrnagy
Tóth András főhadnagy

Technikai munkatársak/Technical Staff:

Doboczki Ferenc
Konta Sándorné
Molnárné Csősz Irma

Szerkesztő és Webmester/Co-ordinating Editor and Web Manager:

Töreki Ákos főhadnagy

HU ISSN 2061-9499

***

ZMNE BJKMK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-356 mellék)
hirado@zmne.hu

Tartalomjegyzék

Köszöntő

A ***Hírvillám*** megjelenésének alkalmából tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

A Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Híradó Tanszéke sok évtizedes hagyományokra tekint vissza mind az alapfokú tisztképzés, mind a magasabb parancsnoki tisztképzés, mind pedig a tudományos képzés terén. Szakmai kultúránk kiforrott, stabil alapokon nyugszik, oktatási egységünk kollektívája szeretné ezért egyrészről a szakma zászlóshajójának, másrészről olyan integráló erőnek tekinteni önmagát, amely hatékonyan elősegíti a védelmi szférán belüli, illetőleg a védelmi és civil területek közötti gyümölcsöző párbeszédet, a tudástranszfert. Tanszékünk a sok évtized alatt felhalmozott ismereteinek és tapasztalatainak, illetőleg felkészültségének birtokában elérkezettnek látja az időt arra, hogy a közvélemény számára az ágazatban zajló szakmai-tudományos munka révén megszülető szellemi termékek közzétételének lehetőségét érdemben is bővítse.

Tudományos időszaki kiadványunk első számának megjelentetését jeles napra datáltuk, hiszen a mai napon, születésének 208. évfordulóján ismételten megemlékezünk karunk névadójának, Bolyai János világraszóló munkásságáról és annak eredményeiről. Dicső katona-tudós elődünk nyomdokain lépkedve kiadványunkkal tehát célunk, hogy a Katonai Műszaki Doktori Iskola és a Hadtudományi Doktori Iskola tagjainak, valamint a távközléssel, katonai híradással, informatikával és információvédelemmel foglalkozó hazai és külföldi szakemberek számára olyan fórumot biztosítsunk, amely elfogadottságával hitelesen biztosíthatja a tudományos eredmények, publikációk közlését, összefogását és azok szakmai környezetben történő tanulmányozását.

Fenti gondolatok jegyében indítjuk útjának új kiadványunkat, amely évente két alkalommal kerül kiadásra korlátozott példányszámban nyomtatva, valamint elektronikus formában on-line megjelenéssel. A benyújtott cikkek lektorálás után kerülhetnek a kiadványba, így biztosítva annak minőségét és színvonalát.

A kiadvány áttekintéséhez jó időtöltést kívánunk, egyúttal szemléljük bizakodva a jövőt, remélve, hogy a Hírvillám a szakmai-tudományos élet mérvadó fórumává válik.

Budapest, 2010. december 15.

Pándi Erik
tanszékvezető

Farkas Tibor – Pándi Erik – Tóth András
farkas.tibor@zmne.hu – pandi.erik@zmne.hu – toth.hir.andras@zmne.hu

A VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÓ- ÉS INFORMATIKAI RENDSZERÉNEK MEGSZERVEZÉSE[1]

Absztrakt

Jelen közlemény ajánlást tesz a Magyar Honvédség külföldi missziójában szolgálatot teljesítő alegységek híradó és informatikai támogatása tárgyában.

This publications presents a proposal on the topic of communication and IT support of units of the Hungarian Army serving in foreign missions.

Kulcsszavak: *katonai műveletek, Magyar Honvédség, missziós tevékenység ~ military operations, Hungarian Defence Forces, missionary activity*

BEVEZETÉS

Az alegységek vezetése a hadművészet legfontosabb alkotóeleme, amely számos kérdést sorakoztat fel, melyek közül kiemelkedik az összeköttetések megszervezése az elöljárókkal, alárendeltekkel és az együttműködőkkel. Az MH Összhaderőnemi Doktrínában a híradás és az informatika a harci támogatás csoportjába tartozik. Ennek egyik szegmense a híradó és informatikai támogatás. A Magyar Honvédség rendeltetéséből adódó feladatai megvalósításának alapfeltétele a korszerű híradó- és informatikai rendszer alkalmazása. Az MH tábori hírrendszere jelenleg csak megközelítőleg képes ellátni a vezetéstámogatási feladatokat, amely jelentősen csökkenti annak hatékonyságát. Nagy gondot okoz a részeiben még analóg technikai eszközök jelenléte, a különböző híradó eszközök közötti interoperabilitás és a nem egységes kommunikációs rendszer hiánya. Mindezek okán több alkalommal került sor arra, hogy a többnemzeti műveletekben résztvevő híradó szakállomány alkalmi jelleggel hárított el felmerülő hibákat, kapcsolási fennakadásokat.

A felvázolt kihívások és missziós képességek nagymértékben behatárolják mindazon paramétereket, melyekkel rendelkeznie kell egy korszerű híradó- és informatikai rendszernek. A hazai gyakorlatok, missziós felkészülések során meg kell vizsgálni mindazon lehetőségeket, amelyek elősegítik a híradó- és informatikai rendszer megszervezését. A válságreagáló műveletek során szerzett hazai tapasztalatok és más szövetséges országok jártassága előmozdítja e szervezési munkákat. Az MH képességi ambíció szintje, amely az ország határain kívül folytatott műveletekben résztvevő alegység méretét határozza meg, elsősorban zászlóalj szintű erőt determinál. Ennek értelmében a válságreagáló műveletekben résztvevő alegységek híradó- és informatikai támogatása elsősorban zászlóalj szintű alegységet kell, hogy kiszolgáljon az országhatáron túli feladatellátás során, a meghatározott egyéb szükséges kiegészítések figyelembevételével. Releváns, hogy a válságreagáló műveletek híradó- és informatikai rendszere biztosítja a parancsnok számára a legátfogóbb, a teljes alkalmazási területre kiterjedő, megbízható és rugalmas kommunikációs hálózatot. Természetesen a szervezésnél figyelembe kell venni az elöljárókkal és az együttműködőkkel történő kapcsolattartást is, amely így teszi teljessé a híradó- és informatikai rendszert. Jelen fejezetben célunk, hogy a NATO által támasztott képességek és az MH nemzetközi

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

tapasztalatainak figyelembevételével rámutassak mindazon követelményekre, amelyek meghatározzák a sikeres műveleteket támogató híradó- és informatikai rendszert, meghatározzuk azokat a tényezőket, amelyek befolyásolják annak megszervezését és bemutassuk a válságreagáló műveleteket támogató híradó- és informatikai rendszer megszervezésének egy lehetséges, elvi folyamatát.

1. A VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÓ- ÉS INFORMATIKAI RENDSZERÉVEL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK, KÉPESSÉGEK

Az eddig rögzítettek alapján, az alegységek folyamatos vezetése és a tevékenység sikere nagymértékben az elöljárókkal, az alárendeltekkel és az együttműködőkkel kialakított permanens összeköttetéstől, információcsere biztosításától függ. Minden esetben meg kell teremteni annak lehetőségét, hogy a parancsok, utasítások, jelentések, intézkedések és egyéb információk mindenkor rendelkezésre álljanak, és garantált legyen a folyamatos összeköttetés, valamint az információk hiteles, megbízható továbbítása. A megszerzett tapasztalatok alátámasztják azt az alapelvet, hogy a folyamatos információcsere csakis valamennyi infokommunikációs eszköz komplex alkalmazásával érhető el, ezért a híradó- és informatikai rendszereknek hálózatalapú (hálózatközpontú) működése központi követelmény. Összességében tehát megállapítható, hogy az eszközök és rendszerek hatékonysága a legtöbb esetben annak függvénye, hogy azokat milyen szinten lehet egy rendszerbe foglalni. Ezért fontos megvizsgálni az ezekkel szemben támasztott követelményeket. A folyamatos információáramlás biztosítása lényeges követelményeket támaszt a híradó- és informatikai rendszerekkel szemben a missziós erők szilárd vezetése érdekében. A Magyar Honvédég Összhaderőnemi Doktrína az alábbiak szerint definiálja a híradással, az informatikával és a híradó- és informatikai rendszerekkel szemben támasztott legfontosabb követelményeket:

- támogassák a vezetést a katonai műveletek teljes keresztmetszetében;
- támogassák a szervezett átmenetet békétől eltérő állapotba;
- biztosítsák az adatok, információhordozó anyagok, továbbítását és terjesztését;
- biztosítsák a riasztási, értesítési adatok továbbítását, a képességet az előrejelzési információk, adatok elemzésére, feldolgozására;
- legyenek képesek a kiválasztott művelet végrehajtásának követésére;
- biztosítsák a megerősítő, támogató erők vezetését, képességeik, anyagi erőforrásaik nyomon követését;
- támogassák a békétől eltérő alkalmazásból békeállapotba történő átmenetet;
- legyenek képesek megvédeni a megszervezett hálózaton áramló információt, fizikailag magát a rendszert. [1]

A dokumentum a híradással és az informatikával szemben támasztott követelmények közül a támogatást, szolgáltatás-nyújtást, az interoperabilitást, az időbeniséget, a prioritások meghatározását, a szilárdságot, rugalmasságot és a biztonságot emeli ki. Véleményünk szerint a fenti megállapítások jól tükrözik a legalapvetőbb követelményeket, de a válságreagáló műveletek híradó- és informatikai támogatása szélesebb körű elemzéseket követel meg a műveleti feladatok összetettsége és az alegységek összetétele miatt. A hadműveleti területeken végrehajtott tevékenységek megkövetelik, hogy a híradó és informatikai központ megszakítás nélkül üzemeljen, biztosítsa a gyors, hatékony és biztonságos információcserét az alárendeltek, elöljárók és az együttműködők között a kiépített híradó- és informatikai vonalak felhasználásával. Az esetenként nagy mennyiségű információk gyors továbbítása korszerű, nagy kapacitású infokommunikációs eszközök együttes alkalmazását igényli. Ennek biztosítása érdekében kiválóan felkészített és kiképzett szakállományra van szükség.

A korszerű kommunikációs rendszerek jellemzője, hogy a haderőnemeknek, fegyvernemeknek, szakcsapatoknak biztosítja a beszéd és adat típusú kommunikációs igényeit; integrálja a rádióhíradást, a vezetékes távbeszélő hálózatot és a műholdas híradást; magas fokú biztonságot nyújt az elektronikus ellentevékenységekkel, felderítéssel szemben minden szinten; az esetleges új igényeknek megfelelően könnyen átszervezhető; és mindez központilag menedzselve megvalósítható. A fent felsorolt követelményeket kiegészítve, a híradó- és informatikai rendszerrel szemben az alábbi kritériumokat, képességeket tartjuk fontosnak.

1.1. A vezetés támogatása minden vezetési szinten, a hadművelet teljes keresztmetszetében

A gyakorlati tapasztalatok alátámasztják, hogy válságreagáló műveletekben résztvevő erők minden szintjén biztosított kell, hogy legyen az összeköttetés. A feladatok hatékony végrehajtása megköveteli ezek kialakítását, beleértve az együttműködő, megerősítő nemzetek katonai alegységeivel és más, nem katonai erőkkel, mivel így érhető el a teljes hadműveleti képesség. A teljes vezetés és irányítás megköveteli, hogy az összeköttetés megvalósuljon a NATO irányába is. Ennek elérése igen nehéz feladat, hiszen a változó összetételű erők és az eltérő infokommunikációs eszközök megnehezítik a sikeres híradó- és informatikai rendszer kialakítását. A vezetés támogatása elérhető a nagy körültekintéssel megtervezett és megszervezett infokommunikációs rendszer kialakításával.

1.2. Együttműködő képesség

A NATO vezette többnemzeti műveletek során, az együttműködés alapfeltétele a kompatibilitás és az interoperabilitás megléte, mert ezek hiányában az előző pontban leírt követelmény sem valósul meg, és ez nagymértékben befolyásolja a hadműveleti vezetés és irányítást, illetve annak kimenetelét. Az interoperabilitás az a lehetőség, amikor a rendszerek, egységek vagy kötelékek szolgáltatásokat nyújtanak más rendszereknek, egységeknek vagy kötelékeknek, egyben szolgáltatásokat fogadnak el egymástól és ezzel lehetővé válik közöttük a tényleges együttműködés [2]. Az interoperabilitás összetevői, mint a technikai, emberi, kiképzés és felkészítési, valamint eljárási módszerek együttesen biztosítják e feltételt.

Az interoperabilitás elérhető a NATO STANAG-ek[2] alkalmazásával az összetevők minden területén, továbbá a közös NATO gyakorlatok végrehajtásával.[3]

A Szövetséges Összhaderőnemi Doktrína (AJP-01) alapján az alábbi feltételeknek kell teljesülnie az interoperabilitás megvalósulása érdekében:

- a rendszer koncepciójának és pontos definíciójának tökéletesítése, valamint a közös működési környezet megteremtése;
- az információ és az adatkezelés kialakításának harmonizálása;
- az egyeztetett hadműveleti, eljárási és technikai szabványok kiadása és végrehajtása;
- közös gyakorlás és gyakorlatok.

2 NATO Standardization Agreement: NATO egységesítési egyezmények, amelyek a Szövetség tagjai közötti biztosítják a technikai, felszerelési, eljárásmódbeli, terminológiai és egyéb területen jelentkező együttműködés egységességét. A NATO STANAG-ek felelőse a NATO Standardization Agency. (NATO Szabványosítási Úgynökség)

3 Ilyen gyakorlat a Combined Endeavor nemzetközi híradó és informatikai interoperabilitási rendszergyakorlat, amelyen NATO, PfP és egyéb meghívott országok vesznek részt. Az MH TD, MH 43. Nagysándor József Híradó és Vezetéstámogató Ezred állománya is részt vesz ezeken az évente megrendezésre kerülő gyakorlatokon.

1.3. Információvédelem és híradó biztonság

A Végrehajtó Erő (IFOR: Implementation Force), a Stabilizációs Erő (SFOR: Stabilisation Force), és az ISAF missziós tapasztalatai mind igazolják, hogy az „ellenség” folyamatosan lehallgathatja a rádióforgalmazásokat, esetlegesen zavarhatja azokat. Ezért missziós tevékenységet támogató híradó- és informatikai rendszer minden esetben a meghatározott szintnek megfelelően kell, hogy kezelje, továbbítsa az adatokat, amely biztosítja mind a személyek, mind a haditechnikai eszközök a védelmét. A biztonság kialakításának legalapvetőbb követelménye, hogy a kommunikációs csatornák előírásoknak megfelelő védettséggel rendelkezzenek a különböző támadásokkal szemben. Az alapvető biztonság elérhető a specifikus rendszabályok meghatározásával és betartásával.

1.4. Magas fokú készenlét, gyors bevethetőség

A magas fokú készenlét biztosítja, hogy a híradó- és informatikai rendszer minden időben és helyzetben képes legyen a vezetés támogatására. A gyors bevethetőség feltételezi a teljes rendszer (eszközök és a kezelő személyzet) magas fokú készenlétét, amely támogatja a híradó- és informatikai rendszer alkalmazását mindennemű katonai művelet során. A magas fokú készenlét elérhető korszerű technikai eszközök és eljárásmódok alkalmazásával, időbeni feladatszabással, és az állomány magas szintű felkészítésével.

1.5. Rugalmasság és reagáló képesség

A híradó- és informatikai rendszer azon tulajdonsága, hogy megváltozott körülmények között képes biztosítani a hálózatok eredeti rendeltetésétől eltérő alkalmazását az új követelményeknek megfelelően, illetve képes az azonnali válaszlépésekre, amellyel megfelel az információcserével és feldolgozással szemben támasztott követelményeknek. Fontos, hogy a támogatott erőkkel, szervezetekkel megegyező időben képes végrehajtani az áttelepülési, átszervezési feladatokat. A reagáló képesség biztosítja az alternatív utak, tartalék rendszerek és berendezések előkészítését és fenntartását, azzal a céllal, hogy azonnal helyre tudja állítani az összeköttetést a rendszer, a berendezés kiesése, hibája esetén. A reagáló képesség alapköve a megbízhatóság, a szilárdság és az időbeniség.

1.6. Mozgékonyság

A híradó- és informatikai rendszernek az a képessége, hogy azt rövid idő alatt lehet telepíteni, bontani, áttelepíteni és a helyzetnek megfelelően a felépítését megváltoztatni, illetve biztosítja azon erők, hadrendi elemek mobilitását, amelyeket a rendszer támogat anélkül, hogy csökkenne az információcsere és az információfeldolgozás folyamatossága, mennyisége vagy minősége. Ez a tulajdonság elérhető a viszonylag egyszerű felépítésű rendszer kialakításával, amely a gyors telepítést is eredményezi. Természetesen a műveletek többnemzeti jellege, a nagy távolságok és a szélsőséges időjárási és földrajzi viszonyok nem minden esetben teszik ezt lehetővé. A mobilitás tartalmazza az első fejezetben leírtaknak megfelelően a rendszer minden elemének azon képességét, hogy támogatja a különböző szállítási típusokat (vízi, légi, szárazföldi).

A válságreagáló műveleteket támogató híradó- és informatikai rendszernek ez a tulajdonsága kiemelten kezelendő, mivel az országhatáron kívüli műveletek összetett logisztikai szállítást igényelnek.[4]

4 A francia fegyveres erők CIS technikai eszközei támogatják a különböző szállítási típusokat, amellyel biztosítják a teljes rendszer kitelepítését az adott hadműveleti területre. Egy példával bemutatva: A gépjárművek, amelyek a híradó- és informatikai konténereket szállítják, alkalmasak a légi szállításra, mivel a teljes felépítmény olyan méretű, amely biztosítja a szállító repülőgép rakterében történő elhelyezését.

1.7. Moduláris felépítés

A különböző típusú műveletek eltérő hadrendi felépítést, eljárásokat és vezetést igényelnek. Ennek megfelelően a híradó- és informatikai rendszernek is támogatnia kell mindennemű műveleti feladatot, amely elérhető a teljes híradó- és informatikai rendszer moduláris felépítésével. A moduláris felépítés lehetővé teszi, hogy a teljes rendszer, a szervezés vagy átszervezés folyamán a hadműveleti igényeknek megfelelően tetszőleges részegységekkel kialakítva kerüljön összeállításra. Jelen képesség fontosságát jól tükrözi az MH Könnyű Gyalog Század mandátumának lejárta, amely során a híradó-technikai eszközeinek egy része beintegrálásra került az MH PRT híradó- és informatikai rendszerébe. Ennek alapfeltétele a kompatibilitás és az interoperabilitás, illetve a pontos hadműveleti feladat meghatározása.

Különböző információs rendszerek támogatása (hálózatalapú működés)

A híradó- és informatikai rendszer azon tulajdonsága, hogy képes együttműködni a hadműveleti vezetést támogató egyéb információs rendszerekkel. Az előzőekben leírtaknak megfelelően, ez a képesség biztosítja azt, hogy valamennyi infokommunikációs eszköz és rendszer (NNEC: NATO Network Enabled Capability, Network-Centric Warfare képesség alapján, C4ISR, C2, C3 rendszerek, stb.) komplex alkalmazásával legyen támogatott a vezetés és irányítás.

1.8. Könnyen továbbfejleszthető

A híradó- és informatikai rendszer megszervezésénél figyelembe kell venni, hogy az esetleges változások hatására könnyen, viszonylag kis költséggel továbbfejleszthető legyen. Ez az alkalmazásra és a rendszer beszerzésre egyaránt vonatkozik. Az első fejezetben meghatározott fejlesztések és a kezdeti kialakítások során minden esetben figyelembe kell venni, hogy az infokommunikációs eszközök és eljárások gyors valamint költséghatékony modernizációja csak és kizárólag továbbfejleszthető rendszerek alkalmazásával érhető el.

Hálózatfelügyelet és hálózatmenedzsment biztosítása

A hálózatmenedzsment és a hálózatfelügyelet legnagyobb szerepe a híradó- és informatikai rendszerek megszervezése és üzemeltetése során jelentkezik. Meglátásunk szerint ez a képesség egy komplex hálózatot alkotó több rendszertechnikai elem és hálózat rendszerbe történő szervezését és annak felügyeletét biztosítja, amely elosztott adatbázison alapul. A felügyelet a hálózati elemeket és munkaállomásokat szervezi, és automatikusan figyeli, amely különböző hardveres és szoftveres elemek felsorakoztatásával segíti a rendszerfelügyelők tevékenységét.

A megszerzett tapasztalatok alátámasztják mindazon alapelveket, hogy a parancsnok számára - a vezetési és irányítási munkája érdekében - biztosítani kell a lehetőség szerinti legnagyobb mennyiségű, minden területre kiterjedő (felderítési információk, saját csapatok helyzete, stb.) információkkal történő ellátást, és az elöljárók irányába a folyamatos és megbízható jelentések továbbításának feltételét.

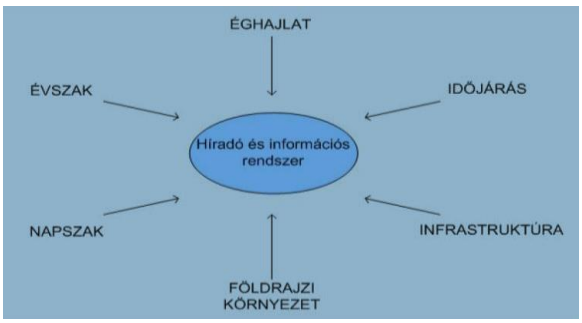
A többnemzeti NATO válságreagáló műveletekben résztvevő koalíciós erőkkel szemben támasztott követelmények, és a kitűzött cél elérése érdekében meghatározott feladatok determinálják a híradó- és informatikai rendszer képességeit.

A nagy mennyiségű információk gyors továbbítása korszerű, nagy kapacitású infokommunikációs eszközök együttes alkalmazását, rendszerbe szervezését igényli, amely hálózatalapú működést biztosít.

A felsorolt és megfogalmazott követelmények teljesítése esetén képes a híradó- és informatikai rendszer támogatni a válságreagáló műveleteket a hadművelet teljes spektrumában.

2. A VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÓ- ÉS INFORMATIKAI TÁMOGATÁSÁT BEFOLYÁSOLÓ TÉNYEZŐK

Az előző alfejezetben megfogalmazott, a válságreagáló műveleteket támogató híradó- és informatikai rendszer képességei, valamint a támogatás megszervezését befolyásoló tényezők megismerése, figyelembe vétele határozza meg azt az alapvető irányvonalat, amely segítségével létrehozható a vezetés és irányítást támogató híradó- és informatikai rendszer. Egyértelmű és vitathatatlan, hogy a híradó- és informatikai támogatás megszervezése az adott műveleti helyzettől, a tevékenység jellegétől, a vezetési igényektől függ. Mindezek mellett, fontosnak tartjuk alapos vizsgálat alá vetni minden részterületet, hogy a legmegbízhatóbb, minden vezetési igényt kielégítő, megbízható és szilárd rendszert lehessen létrehozni. Magyar Sándor doktori értekezletében megfogalmazta azokat az emberi és környezeti tényezőket, amelyek jelentős hatást gyakorolnak a híradásra. „ A sikeres eredményes munkához a szellemi, szakmai felkészültség mellett fontos a megfelelő fizikai erőnléti állapot, a fizikai alkalmasság. […] A missziós területen a híradó katonákat is megviselik az egyéni felszerelések viselése […] valamint a jelentős hőmérséklet különbség. […] A külső környezeti tényezők (fizikai dimenziói) missziókra gyakorolt hatása jelentősen befolyásolja a szolgálatot teljesítő állomány tűrőképességét. […] A tevékenységi terület elhelyezkedése, terep, évszak, napszak, időjárásmind-mind hatással vannak a katonai művelet végrehajtásának híradó és informatikai biztosítására.” [3]



1. ábra: A híradást befolyásoló külső tényezők
Forrás: [4]

A híradó- és informatikai rendszer megszervezésekor fontos figyelembe venni az európai hadszíntértől merőben eltérő földrajzi, éghajlati hatásokat, amelyek nagymértékben befolyásolják a személyzetet, az infokommunikációs eszközöket. Mindezeken túlmenően alapos vizsgálatot kell végrehajtani annak érdekében, hogy minden hatástényező meghatározható legyen, amely befolyásolja a rendszer kialakítását.

2.1. A hadműveletei erők sajátos összetétele (többnemzeti jelleg)

A többnemzeti műveletek során az előző alfejezetben leírtaknak megfelelően, meg kell határozni azokat a kommunikációs csatornákat és információs eljárásokat, amelyek képesek kiszolgálni a vezetés és irányítást. A rendszert alkotó technikai eszközök kiválasztása nagy körültekintést igényel, figyelembe véve az elöljárókkal és az együttműködőkkel történő kapcsolattartást. Jó példa erre az iraki többnemzeti művelet, amely során az MH SZZ a lengyel vezetésű hadosztály alárendeltségében működött, vagy az ISAF, ahol német irányítás

alatt teljesít szolgálatot a magyar kontingens. Megfigyelhető, hogy a jelenleg is folyó többnemzeti műveletek katonai, rendőri, civil és politikai tevékenységeket és erőket egyaránt tartalmaznak, amelyek jelentős hatást gyakorolnak a híradó- és informatikai rendszer technikai összetételére valamint a szervezési, tervezési eljárásmódokra. A többnemzeti jelleg meghatározza azokat az alapvető technikai eszközöket, eljárásmódokat és követelményeket, amelyek biztosítják az együttműködést a résztvevő erőkkel.

2.2. Komplex feladatrendszer

A feladatrendszer minden válságreagáló művelet esetében igen összetett, de az adott nemzetek gyakran csak részfeladatokra specializálódnak[5], amely megkönnyítheti a híradó- és informatikai rendszer kialakítását. Azonban jó ellenpélda az MH PRT, ahol igen sokrétű és szerteágazó rendeltetésű erő számára kell biztosítani infokommunikációs támogatást. Természetesen az egyes részfeladatok megegyezhetnek, ezért véleményünk szerint kiemelten fontos a moduláris felépítésű híradó- és informatikai rendszer, amely alapelemei feladatorientáltan bővíthetők, kiegészíthetők a megkövetelt speciális összetevőkkel. A feladatrendszer nagymértékben meghatározza, hogy milyen mértékben kell rádió-, vezetékes-, LOS-, műholdas összeköttetéseket tervezni és alkalmazni, mely feladatokat lehet támogatni ezekkel az összeköttetési formákkal. Ezért nagy figyelmet kell fordítani a különböző eszközök alkalmazásának előnyeire, hátrányaira. Az alábbi ábrán felsoroltuk azokat a legalapvetőbb tulajdonságokat, amelyeket figyelembe kell venni a tervezés során.

ÖSSZEKÖTTETÉS TÍPUSA	ÖSSZEKÖTTETÉS ELŐNYE	ÖSSZEKÖTTETÉS HÁTRÁNYA
RÁDIÓ	♣ GYORS ÖSSZEKÖTTETÉS LÉTESÍTÉSE ♣ MENET KÖZBEN IS ALKALMAZHATÓ ♣ ELLENSÉGES ERŐKÖN KERESZTÜL IS HASZNÁLHATÓ ♣ PONT- MULTIPONT KÖZÖTTI ÖSSZEKÖTTETÉST IS BIZTOSÍT	♣ KÖNNYEN ZAVARHATÓ, BEMÉRHETŐ, LEHALLGATHATÓ ♣ IDŐJÁRÁS, NAPSZAK, DOMBORZAT ZAVARÓ HATÁSA
VEZETÉKES	♣ NEHEZEN LEHALLGATHATÓ ♣ ZAVARÁLLÓ ♣ NAPSZAAK, ÉVSZAK, DOMBORZAT NEM BEFOLYÁSOLJA AZ ÖSSZEKÖTTETÉST	♣ LASSÚ TELEPÍTÉS ♣ NAPSZAK, ÉVSZAK, DOMBORZAT BEFOLYÁSOLJA A TELEPÍTÉST ♣ MOZGÁSBAN NEM ALKALMAZHATÓ
LOS	♣ NAGY TÁVOLSÁG ÉS SÁVSZÉLESSÉG ♣ TÖBBCSATORNÁS ÖSSZEKÖTTETÉS ♣ KEVÉSBÉ LEHALLGATHATÓ (IRÁNYÍTOTT ANTENNA)	♣ DOMBORZATFÜGGŐ ♣ RÁLÁTÁS SZÜKSÉGES ♣ TELEPÍTÉSI HELY MIATT SEBEZHETŐ ♣ IDŐJÁRÁSRA ÉRZÉKENY
MŰHOLDAS	♣ ÁLLÓHELYBEN MOZGÁSBAN EGYARÁNT BIZTOSÍT ÖSSZEKÖTTETÉST ♣ KEVÉSBÉ DOMBORZATFÜGGŐ ♣ BÁRHOL HASZNÁLHATÓ A VILÁGON ♣ NAGY SEBESSÉGŰ ÖSSZEKÖTTETÉS ♣ MEGBÍZHATÓ	♣ KÖLTSÉGES

2. ábra: A különböző összeköttetés típusok legfontosabb tulajdonságai

A hadműveleti terület elhelyezkedése, a műveletek mérete, kiterjedése

A műveleti terület mérete jelentős hatást gyakorol az infokommunikációs koncepcióra. A nagy kiterjedésű többnemzeti műveletben szerepet vállaló kontingens támogatását nagy kiterjedésű, összetett rendszer tudja csak kiszolgálni, amelynek biztosítania kell a

5 Az MH SZZ szállítási feladatokat látott el Irak területén, míg az MH ŐBZ őrzési és biztosítási feladatokat a KFOR misszióban.

hadműveleti terület, a hátország, és egyéb meghatározott irányok összeköttetését. A műveleti zóna mérete determinálja az erők nagyságát, amely a kapcsolatok kiterjedését is előírja. Kiemelten kell kezelni a honi kapcsolattartást, mivel a hátország és a műveleti terület közötti távolság (és a meglévő infrastruktúra) behatárolja a felhasználható eszköztípusok rendszerbe állítását.

2.3. A többnemzeti műveletek vezetésének szintje

A válságreagáló műveletek olyan politikai, katonai, civil tevékenységeket sorakoztat fel, amelyek nem minden esetben láthatók előre, ezért hatékony irányítást követel meg a vezetés és irányítás minden szintjén. A rendszernek minden esetben támogatni kell a különböző vezetési szinteket. A műveleti feladatok megkezdése előtt központi meghatározásra kerülnek azok a vezető szervek, elöljárók, amelyek a saját erőnket irányítják, ezáltal fel kell készíteni a rendszert az azokhoz való kapcsolódásra. A műveletek folyamán a „vezetési struktúrában" bekövetkező esetleges változásokat minden esetben figyelembe kell venni, a rendszernek követnie kell azt. Az így kialakuló változásokat az összeköttetésekben folyamatosan figyelemmel kell kísérni, meg kell változtatni, amelyet a tervezési időszakban végrehajtott tartalékképzés is biztosíthat.

2.4. A műveleti területen jelenlévő kommunikációs infrastruktúra

A műveleti területen megtalálható infrastruktúrák felhasználása az alkalmazási területen belül és a felső szintű vezető szervek között szükségessé válhat. A szervezés és tervezés fázisában meg kell vizsgálni a meglévő infrastruktúra állapotát, felhasználásának és az ahhoz történő csatlakozásnak a lehetőségét. Az eddigi tapasztalatok azt bizonyítják, hogy legtöbb esetben a válságreagáló műveletet megelőző hadmozdulatban megsemmisül a helyi infokommunikációs hálózat, vagy egyáltalán nem is volt kiépítve (vagy nem megfelelő fejlettségű). Egyes esetekben a műveleti területeken civil kommunikációs szolgáltatók megjelenését és saját hálózatuk kiépítését követően, felhasználhatóvá válnak az új kommunikációs hálózatok[6], amely fő bázisát vagy tartalékát képezheti egyes összeköttetési vonalaknak. Amennyiben felhasználható a polgári kommunikációs infrastruktúra, elemezni kell a polgári és a saját katonai eszközök, hálózatok csatlakoztatásának alternatíváit.

2.5. A rendelkezésre álló idő és a küldetés várható időtartama

A híradó- és informatikai rendszer megszervezéséhez rendelkezésre álló idő adott esetben igen lerövidülhet, amennyiben azonnali beavatkozást igénylő válságkezelésére kerül sor. Természetesen ennek igen kis esélye van, mivel a NATO rendelkezik erre az esetre felkészített erőkkel.[7] Nyilvánvalóan a rendelkezésre álló idő a megszervezett, telepített és üzemeltetett híradó- és informatikai rendszer átszervezésére is hatást gyakorol. Az időtényező meghatározza azt az időintervallumot, amely rendelkezésre áll, hogy az

6 Roshaan; AWCC; THALES

7 „ a. NATO közvetlen alárendeltségében lévő erők, amelyek folyamatos készenlétben vannak
b. NATO Reagáló Erő, amely igen gyorsan (5-30 nap) bárhol bevethető expedíciós képességekkel rendelkezik és már békében valamelyik NATO parancsnokság alárendeltségébe tartozik;
c. NATO bevethető (telepíthető) (0-90 nap) magas készenlétű erők, amelyek válthatják, illetve kiegészíthetik az expedíciós erőket és ezzel valamelyik NATO parancsnokság alárendeltségébe kerülhetnek;
d. NATO bevethető (telepíthető) (91-180 nap) alacsonyabb készenlétű erők, amelyek válthatják, illetve kiegészíthetik a magasabb készenlétű, bárhol telepíthető erőket és ezzel valamelyik NATO parancsnokság alárendeltségébe kerülhetnek;
e. EU reagáló erők, amelyek az EU gyorsreagáló erői harccsoportjainak megalakításához (amely magába foglalja 15 napon belül a műveleti területre való kiérkezést) kapcsolódnak." [5]

esetlegesen bekövetkezett hadrendi és egyéb változásoknak megfelelően átalakításra kerüljön a híradó- és informatikai rendszer. A küldetés várható időtartama alapján meg kell vizsgálni a rendszer felépítésének lehetőségeit. Amennyiben rövid idejű berendezkedés várható, elsősorban könnyen telepíthető (bontható, áttelepíthető), főként vezeték nélküli technológián alapuló összeköttetéseket kell tervezni. Természetesen a küldetés várható időtartama a legnehezebben meghatározható összetevő, így a moduláris felépítés és a rendszer rugalmasságára támaszkodva kell megszervezni a támogató rendszert.

2.6. A meglévő katonai hálózatok felhasználása

A híradó- és informatikai rendszer megszervezése és megtervezésekor figyelembe kell venni a már esetlegesen telepített katonai infokommunikációs hálózatokat. Amennyiben rendelkezésre áll ilyen hálózat, mérlegelni kell annak felhasználási lehetőségét, illetve az ahhoz történő csatlakozás alternatíváit. A műveletek során a NATO által telepített hálózatok mellett előfordulhat, hogy egy másik szövetséges erő által – amely befejezte a feladatainak ellátását a térségben – létesített, telepített hálózat is rendelkezésre áll.[8] Természetesen ezt az „opciót" is figyelembe kell venni, és ekkor ismét előtérbe kerül az interoperabilitás kérdése. A számítógépes (informatikai) hálózatok esetén ezeknek a hálózatoknak az alkalmazásra történő átvétele egyszerűbb, könnyebben megvalósítható, hiszen a civil életben is megtalálható vezetékek, egyéb eszközök (router, switch) kerülnek – többnyire – felhasználásra, így biztosítva a kompatibilitás kérdését.

2.7. Áramellátás

A válságreagáló műveletek híradó- és informatikai rendszere tervezése során meg kell vizsgálni a működtetéséhez szükséges feltételeket. Ennek egyik „kulcskérdése" az áramellátás. Fel kell készülni azokra a lehetőségekre, amelyek szavatolják az eszközök működéséhez szükséges elektromos áramot. Természetesen a híradó komplexumok, állomások rendelkeznek saját aggregátorokkal, de a települési hely (vezetési pont) villamos energiával történő ellátására tervet kell készíteni az adott terület infrastruktúrájának megfelelően. Amennyiben ez rendelkezésre áll, tovább kell elemezni a megbízhatóság, sebezhetőség, folytonosság és egyéb technikai paraméterek perspektívájából.

Elektronikai hadviselés[9] elleni védelem

A teljes híradó- és informatikai rendszert fel kell készíteni az elektronikai ellentevékenységekkel szembeni védelemre, a lehető legnagyobb mértékben le kell csökkenteni annak sebezhetőségét. A vezetés és irányítás folytonosságának, megbízhatóságának és biztonságának megőrzésében fontos szerepet tölt be ez a szakterület, amelyet megfelelően felkészített szakemberek látnak el. Mérlegelni kell az ellenség képességeit (zavarás, felderítés, lehallgatás) a felderítési, hírszerzési információkara alapozva, majd szervezési rendszabályokkal és technikai eszközökkel kell biztosítani a védelmet, csökkenteni az ellenséges zavarás hatékonyságát. Bár az eddigi tapasztalatok alapján, a válságreagáló műveletek során nem várható jelentős ellentevékenység ezen a téren, de az „ellenség" folyamatos fejlesztései, új eljárásai (még ha azok elmaradottabbak a fejlett

8 Az MH PRT miután átvette a tartomány irányítását a holland féltől, az általuk kiépített informatikai, távközlési elemek egy része került alkalmazásra a magyar fél részéről.

9 „Az elektronikai hadviselés az elektromágneses spektrumot hasznosító azon katonai tevékenység, amely magában foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, valamint az irányított energiát is beleértve az elektromágneses energia felhasználását abból a célból, hogy megakadályozza, vagy korlátozza az ellenség részéről az elektromágneses spektrum hatékony használatát, és lehetővé tegye annak a saját csapatok általi használhatóságát." [7]

katonai eszközökhöz, eljárásmódokhoz képest) jelentős hatást gyakorolhatnak a kiépített és üzemeltetett rendszerre. A technikai eszközök fejlődésével egyre több lehetőség kínálkozik az infokommunikációs rendszerek zavarására, és egyre szélesebb körű azoknak a rendszereknek, eszközöknek a száma, amelyekkel támadásokat lehet indítani. „[…] olyan perspektivikus területek léphetnek be az elektronikai hadviselés fegyvertárába, mint a mobil hálózatok zavarása, a helymeghatározó rendszerek zavarása, az impulzusbombák és nagyenergiájú rádiófrekvenciás fegyverek, a számítástechnikai rendszerek, eszközök elleni támadás eszközei, a lézer eszközök és az ezeket hordozó modern platformok.” [6]. Mindezek mellett meg kell jegyezni, hogy nagy problémát jelent a többnemzeti műveletekben a rádióeszközök zavarása, amely jelentős hányadát a kölcsönös-, a légköri-, és a helyi elektromos zavarok teszik ki, amelyre megfelelő menedzsmenttel és körültekintő szervezéssel kell felkészülni. Tehát a technikai eszközök és az élőerő védelme érdekében fel kell készülni a saját csapatok, a helyi infrastruktúra és az ellenség által keltett azon behatásokkal szemben, amelyekkel csökkenteni, rombolni akarják a vezetés és irányítási képességünket.

2.8. Információs rendszerek támogatása

A híradó- és informatikai rendszerek előzőekben felsorolt tulajdonságai, követelményei közül a hálózatalapú működésnek megfelelően, figyelembe kell venni a szervezés folyamán a különböző információs rendszereket, amelyek üzemelnek a válságreagáló műveletek során. A rendszerek közötti átjárhatóságot, kapcsolatot meg kell teremteni a szilárd és hatékony vezetés és irányítás támogatása céljából.

2.9. Kezelő állomány kiképzettsége és felkészültsége

A nemzetközi környezetben szolgálatot teljesítő kontingensek híradó- és informatikai (információvédelmi) felkészítése összetett feladat. Minden szakbeosztású katonának ismernie kell a technikai eszközöket és a megszervezett komplex rendszert. A felkészítésnek ki kell terjednie a vezetékes- és vezeték nélküli összeköttetési formák megszervezésére, alkalmazására, és a híradó- és informatikai eszközök kezelésére, szolgáltatásainak ismertetésére illetve az alapvető hibaelhárításra. A felkészítést nagymértékben befolyásolja a már megszerzett tapasztalatok feldolgozása, és azok átadása az állomány részére. A követelmények és képességek magas szintű ismerete és elsajátítása alapeleme a híradó- és informatikai rendszer sikeres működésének. A felkészítésnek és kiképzésnek főbb követelményeit Koronczai Tibor a következőképpen határozta meg: „A jelenleg folyó és a jövő várható műveletei egyértelműen meghatározzák a missziókhoz és EU katonai képességeihez hozzájáruló erők felkészítésének, kiképzésének főbb követelményeit, melyek a következők:

- összhaderőnemi, integrált felkészítés, kiképzés;
- többnemzeti környezetben való alkalmazási képesség;
- erők és eszközök expedíciós jellege, képessége;
- rendelkezésre állás képessége;
- professzionális, multifunkcionális képességek;
- erősen motivált személyi állomány;
- erős testületi kohézió, testületi szellem;
- parancsnokok vezetői képességeinek fejlesztése.” [8]

Mindezek alapján a válságreagáló műveletek erőinek szakfelkészítése és kiképzése komoly kötelezettséget és feladatot támaszt a támogató állományra, amely jelentős hatást gyakorol a megszervezett rendszer üzemeltetésére.

2.10. A rendelkezésre álló eszközök minősége, mennyisége

A híradó- és informatikai rendszer megszervezése és megtervezésekor ismerni kell a rendelkezésre álló híradó-technikai, információvédelmi és egyéb eszközök tulajdonságait, technikai paramétereit. Célszerűnek tartjuk, hogy a szervezés fázisában, egy olyan komplex adatbázis kerüljön felhasználásra, amely tartalmazza az összes felhasználható technikai eszközt így elősegítve a hírrendszer elemeinek összeállítását. Magyar Sándor doktori értekezésében javaslatot tesz egy adatbázis elkészítésére, amely meghibásodás vizsgálatra, tartalékképzésre alkalmazható. „A híradó eszközök, berendezések meghibásodásának vizsgálatára és a későbbiekben a következtetések levonására javasoljuk egy az összes misszióra kiterjedő híradó adatbázis létrehozását.” [9] Véleményünk szerint a jól kialakított adatbázis (a technikai paramétereken kívül tartalmaz együttműködési képességekre vonatkozó információkat is) elősegíti az olyan híradó- és informatikai rendszer megtervezését, amely a többnemzeti válságreagáló műveletekben megfelel a kihívásoknak, képes azt szilárdan és megbízhatóan támogatni.

2.11. Tapasztalatok során levont következtetések

A válságreagáló műveletek során szerzett tapasztalatok összegzése, folyamatos értékelése kulcsfontosságú, amely lecsökkenti az esetleges technikai, szervezési hibák előfordulásának esélyét, illetve a „túlszervezést, túlméretezést”. Az esetleges rádiós összeköttetési hibák, kiesések, a technikai eszközök meghibásodása (a szélsőséges időjárási viszontagságok miatt), vagy a nem megfelelő alkalmazhatóság, mind meg kell, hogy jelenjen egy adatbázisban, amely jó alapját képezheti a későbbi szervezési eljárásnak. A tapasztalat feldolgozó rendszer[10] megvalósításának igénye már korábban megjelent a Magyar Honvédségben más NATO hadseregek mintájára. A tapasztalatok feldolgozása jelenleg is működik, de nem egységes rendszerben, ennek központosítása a további sikeres műveletekben való részvételünk egyik alapvető eleme. Süle Attila és Csabianszki Viktor az alábbiak szerint fogalmazta meg a rendszer megvalósításának igényét: „A tapasztalatok feldolgozása nem új keletű igény. […] A napjainkban jelentkező, a polgári és katonai eszközök koordinált, sok esetben újszerű alkalmazását igénylő kihívások, a jellemzően aszimmetrikus környezet, korunk technikai, információtechnológiai fejlettsége és gyors ütemű továbbfejlődése, a többnemzeti, az összhaderőnemi, az expedíciós szemlélet újszerű követelményt támasztanak a tapasztalatok feldolgozásával kapcsolatban is. […] Mindezek figyelembevételével időszerűvé vált a NATO és az EU műveleti rendjébe illeszkedő nemzeti tapasztalat feldolgozó rendszer kialakítása.” [10]

Az alfejezetet röviden összegezve és értékelve megállapítható, hogy a híradó- és informatikai rendszer megszervezése nagymértékben függ az adott hadműveleti helyzettől, a tevékenység jellegétől és a vezetési igényektől, de széleskörű vizsgálatot követően, és a

10 Lesson Learned magyar megfelelője, amellyel kapcsolatosan jelenleg az MH Műveleti Központ lát el feladatokat, (az MH ÖHP mellett) az alábbiak szerint:

„b) az MH béketámogató, válságreagáló és válságkezelő műveletek előkészítésében való részvétel, a hatáskörébe utalt feladatok előkészítése, szervezése, a végrehajtás irányítása és a tapasztalatok feldolgozása;

c) a szövetségi rendszerben, illetve a különböző nemzetközi szervezetek alárendeltségében, béketámogató, válságkezelő és válságreagáló műveletekben részt vevő szervezetek nemzeti vezetése, amely magában foglalja HM Honvéd Vezérkar főnöki intézkedés alapján a kontingensek és egyéni beosztásúak kiválasztásának és felkészítésének ellenőrzését és felügyeletét, valamint önálló hatáskörben a kitelepülés, a megváltozott műveleti környezet, a visszatelepülés és kiürítés feltételeinek monitoring jelleggel történő folyamatos értékelését, jogi és szakmai koordinálását, a műveleti tapasztalatok feldolgozását, a nemzetközi szervezetek által irányított válságreagáló és béketámogató műveletekben át-alárendelt erők nemzeti felelősségi és hatáskörbe tartozó feladataival kapcsolatos nemzeti és nemzetközi egyeztetések végrehajtását, valamint műveleti feladatok vonatkozásában koordináló tevékenységet; ” [11]

megszerzett tapasztalatok alapján kell megszervezni a válságreagáló műveleteket támogató infokommunikációs eszközöket felsorakoztató rendszert.

A rendszerrel szemben támasztott képességek, követelmények és a megszervezést befolyásoló tényezők szoros kölcsönhatásban vannak, egymást kiegészítve határozzák meg a híradó- és informatikai rendszer megszervezésének folyamatát.

Az általam megfogalmazott legfontosabb tényezők komplex vizsgálatával, a további műveletek során szerzett tapasztalatok feldolgozásával, és a jövőben meghatározásra kerülő új kihívások integrációjával kell végrehajtani a híradó- és informatikai rendszer megszervezését, megtervezését.

3. A VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÓ- ÉS INFORMATIKAI TÁMOGATÁSA MEGSZERVEZÉSÉNEK FOLYAMATA

A válságreagáló műveletek híradó- és informatikai rendszerével szemben támasztott követelmények, és az azt befolyásoló tényezők figyelembevételével kell minden esetben megszervezni a vezetés és irányítás infokommunikációs támogatását. Ki kell alakítani a feladatra szabott, szükséges és elégséges, a NATO-elvárásoknak is megfelelő, együttműködésre és expedíciós műveletekre alkalmas rendszert. A többnemzeti jellegből adódóan a közös eljárásmódok, a NATO szabványok alkalmazása és a folyamatos konzultációk a válságreagáló művelet eredményes végrehajtásának része. A STANAG 5048[11] a korábbi alfejezetben leírt interoperabilitás és kompatibilitás biztosítása érdekében a legalapvetőbb dokumentum, amelyet figyelembe kell venni a szervezés és tervezés során. A kiadvány meghatározza azokat az eljárásmódokat, amelyek alapján meg kell szervezni a híradó- és informatikai rendszert, illetve azok kapcsolatának minimális mértékét. Az alapvető koncepció szerint biztosítani kell a kapcsolatot az elöljáró és az alárendeltek között, a támogató és a támogatottak között, valamint a szomszédos erők között a harctéren. A megkövetelt kapcsolatok létesítésének felelőssége minden esetben az elöljárótól az alárendelt felé, a támogatótól a támogatott felé; a bal egységtől a jobboldali egység felé.

Természetesen a kapcsolat létesítésének feltételei a fent leírtak szerint valósul meg, de az alárendelteknek lehetőség szerint biztosítaniuk kell az összeköttetés kiépítésének feltételeit. A STANAG 5048 a legalapvetőbb szabvány, de számos más, a Szövetség által kiadott eljárás, szabály, szabvány adhat iránymutatást a saját nemzeti okmányaink, utasításaink mellett, amely alapján meg kell szervezni az összeköttetéseket. A híradó- és informatikai rendszer megtervezését az elöljáró intézkedése alapján kell végrehajtani. Első lépéseként a feladatrendszer, a végrehajtó erők és a műveleti terület figyelembevételével meg kell határozni a híradó- és informatikai rendszer kiterjedését, alapvető összetételét. Az összeköttetések jellegének fő meghatározója a vezetés és irányítás struktúrája nemzeti és többnemzeti szinten. Az elöljárók (mind nemzeti, mind hadműveleti) elhatározása a végrehajtandó feladatra, a műveleti tevékenységre, alapvető irányvonalat ad az összeköttetések létesítésére, a híradó- és informatikai rendszer összetételére. Az elhatározásnak a rendszer megtervezése szempontjából tartalmaznia kell az alábbiakat:

- a feladat célját;
- a művelet vezetési rendszerét (a saját erőnkkel összefüggésben);
- a műveleti feladat típusát, a végrehajtásra kerülő egyéb részfeladatokat;
- a műveleti terület kiterjedését, a hadműveleti körzetet;
- a végrehajtásra létrehozott erő méretét és összetételét;
- a műveletek megkezdésének idejét, időtartamát;
- az esetleges együttműködő, más nemzetek felajánlott alegységeivel kapcsolatos információkat;

11 A NATO szárazföldi csapatok híradó és informatikai rendszerei kapcsolatának minimális mértéke (STANAG 5048)

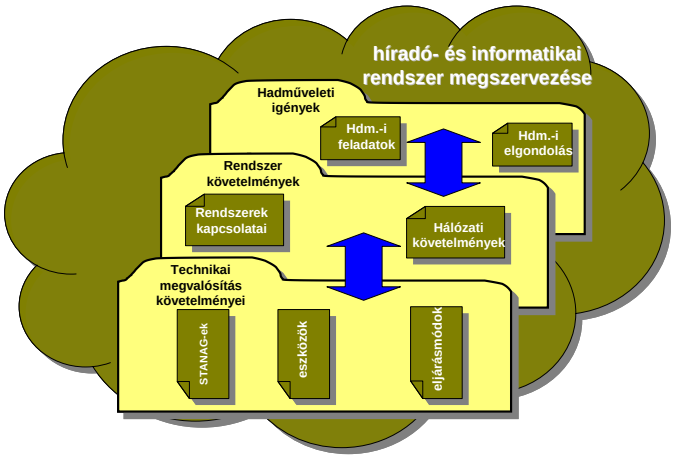
- nem kormányzati szervezetek, egyéb nem katonai szervezetekkel való együttműködést;
- az ellenséges erők várható képességeit.

Az általános műveleti követelmények determinálását követően, annak megfelelően, a második fázisban az azt támogató és minden területet kiszolgáló híradó- és informatikai rendszerstruktúrát is ki kell alakítani, a vezetés és irányítás megvalósítása érdekében. Az alapvető feladatokat figyelembe véve meg kell határozni:

- a híradó- és informatikai feladatrendszert;
- a kapcsolatok követelményrendszerét;
- az összeköttetést a nemzeti (hazai) elöljáróval;
- az összeköttetést a hadműveleti elöljáróval;
- a kapcsolatokat a NATO irányába;
- az összeköttetést az együttműködő katonai erőkkel, polgári szervezetekkel; esetleges rendőri csoportokkal;
- a hadműveleti kapcsolatokat;
- települési helyen (táboron) belül;
- hadműveleti feladatok végrehajtása során;
- a Futár- és Tábori posta híradást, és a logisztikai utánpótlás rendszerét;
- az előzőekből következően a híradó és informatikai eszközök összetételét;
- a híradó és informatikai beosztású személyi állomány összetételt;
- a híradó és informatikai rendszer okmányrendszerét;
- a személyi állomány szakmai felkészítésének rendszerét.

A hadműveleti követelményrendszer meghatározásából következik a híradó- és informatikai feladatrendszer, amely az általános követelményeket sorakoztatja fel. Az előző fejezetekben leírtaknak megfelelően, az infokommunikációs rendszernek tehát támogatnia kell a vezetés és irányítást a művelet teljes spektrumában az alárendeltek és az együttműködők irányában.

A híradó- és informatikai rendszer kialakítását a hadműveleti igények, a rendszer követelmények és a technikai megvalósítás hármas egysége határozza meg, amelyek egymással szoros, elválaszthatatlan kapcsolatban állnak. A három részterület egymást meghatározva, a folyamatos visszacsatolás elvét követve adja meg a műveleteket támogató rendszer felépítését.



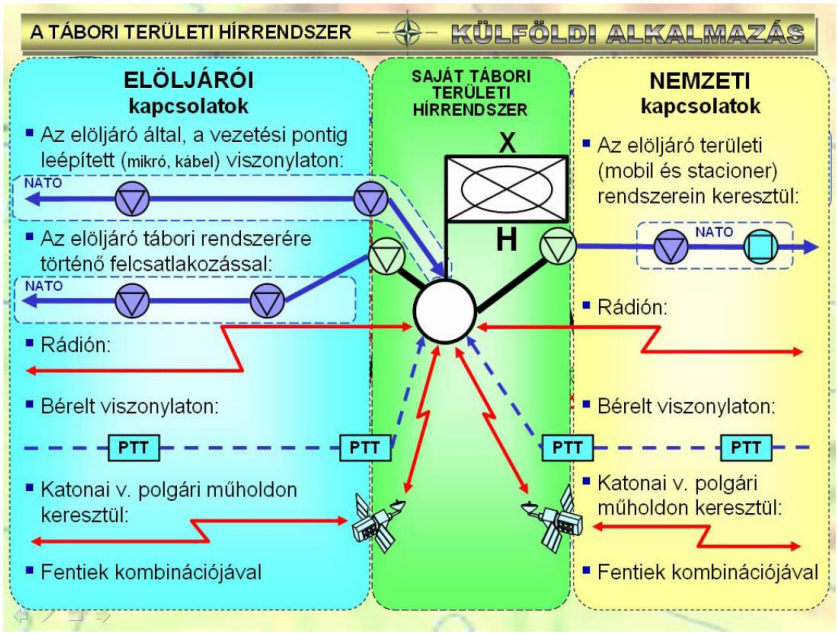
3. ábra: A híradó- és informatikai rendszer kialakításának elve

A hadműveleti igények tartalmazzák azokat a feladatokat, tevékenységeket, amelyek támogatását a rendszernek ki kell szolgálnia. A rendszer követelmények meghatározzák a műveletekben alkalmazott rendszereket és a közöttük lévő kapcsolatokat. A technológiai megvalósítás kritériumai leírják azokat az eszközöket, eljárásmódokat, szabványokat, amelyek alkalmazásra kerülnek. A rendszer megszervezésekor a fentről lefelé elv alkalmazását kell követni, de az elemek kölcsönhatása megköveteli a folyamatos visszacsatolást, illetve az esetlegesen bekövetkezett változások figyelemmel kísérését.

A hazai, nemzeti elöljáróval való kapcsolattartás megszervezésekor figyelembe kell venni a műveleti terület és Magyarország közötti távolságot, terepviszonyokat. A NATO és a hazai többnemzeti műveletek megerősítik, hogy ezen összeköttetés legmegfelelőbb, legmegbízhatóbb módja[12] a műholdas kapcsolat kialakítása. Amennyiben van rá lehetőség, fel lehet használni a NATO stacioner és a polgári távközlő hálózatokat egyaránt. A híradó- és informatikai rendszerek megszervezésekor fontos, hogy minden összeköttetéshez hozzá kell rendelni egy tartalék kapcsolatot, amely az elsődleges kiesése esetén biztosítja a folyamatos vezetést. Másodlagos kapcsolattartási mód lehet az RH rádióeszközökkel szervezett rádióforgalmi rendszer, esetlegesen a GSM szolgáltatók által biztosított mobiltelefon hálózat. Természetesen ezek csoportosítására is szükség van a megbízható, folyamatos összeköttetés érdekében.

A NATO- és a hadműveleti parancsnoksággal történő kapcsolattartás megszervezéséért a STANAG 5048 értelmében – az összeköttetést az elöljárótól az alárendelt irányába kell megszervezni – az elöljáró a felelős. A híradó- és informatikai szakállománynak fel kell készülnie a rendelkezésre álló eszközök, vagy az általa biztosított infokommunikációs eszközök alkalmazásával a kapcsolatok megvalósítása feltételeinek biztosítására. Az egyéb alkalmazott, hálózat nyújtotta képességen alapuló rendszerekre ugyanezen elv vonatkozik. Az összeköttetések módját az elöljáró határozza meg a rendelkezésre álló hálózatok figyelembevételével, amely lehet LOS-; rádiós-; műholdas-; illetve vezetékes kapcsolat. Az együttműködők viszonylatában szintén az alapdokumentum ad iránymutatást, illetve az elöljáró által kiadott intézkedés.

12 „A híradás mód szerinti kategorizálása nem jelent mást, mint az alkalmazott jel, eszköz és terjedési közeg alapján történő megkülönböztetést. A híradás felosztása azon aspektus alapján, hogy a kommunikációra, távközlésre használt eszköz az információ továbbítása érdekében, milyen módszert és terjedési közeget használ fel.” [13]



4. ábra: A külföldön alkalmazott tábori területi hírrendszer NATO és nemzeti kapcsolatai
Forrás: [12]

A hadműveletek vezetésének támogatása a legösszetettebb szervezési, tervezési feladatot eredményezi. Az eltérő műveletek, földrajzi és éghajlati viszonyok jelentős mértékben korlátozzák a lehetőségeket, és alapjaiban határozzák meg az összeköttetések módját. A missziós műveletek során levont következtetések alapján, a feladatokat (járőrözés; konvojkísérés; felderítői tevékenységek; CIMIC feladatok) ellátó alegységek és a vezetési pont (tábor) közötti kapcsolatot rádiós-, illetve műholdas összeköttetéssel lehet megvalósítani. Ennek értelmében, a szervezés időszakában meg kell határozni azokat az alapvető kapcsolatokat, amelyek biztosítják a támogatását a hadműveleti feladatoknak. A kommunikációs összeköttetések mellett meg kell valósítani a rendelkezésre álló hálózatközpontú műveleteket támogató rendszerek hálózatba történő integrálását. A „blue force tracking" alkalmazása, a különböző szenzorok, UAV-k [14] által biztosított információk rendszerbe történő integrálása nélkülözhetetlen az egységes hadműveleti helyzet és a hadműveleti vezetés megvalósításának érdekében. Minden esetben számításba kell venni, hogy az előre nem látható tevékenységeket is támogatnia kell a kialakított híradó- és informatikai rendszernek a megfelelő változtatások végrehajtásával, amely a modulrendszerű felépítés alapján valósítható meg. A vezetési pont (tábor) híradó és informatikai központ releváns az információk fogadásának, továbbításának, védelmének és feldolgozásának folyamatos biztosításában, a híradó- és informatikai rendszer rendeltetésszerű üzemeltetésében. Az elkészült híradó és informatikai terv alapján kell telepíteni és üzemeltetni a rendszert, amely tartalmazza az információk továbbítási rendjének meghatározását, a kapcsolatok megtervezését, az állomány feladatait, az időtényezők meghatározását, a védettség, biztonság rendszabályainak foganatosítását és a belső összeköttetéseket. A törzsek, részlegek és a parancsnokok számára biztosítani kell mindazon összeköttetési formákat, híradó és informatikai eszközöket, amelyek a feladataik végrehajtását támogatják, elősegítik a vezetést.

Az FTP híradást és a logisztikai támogatást az eddigi missziós tevékenységünk során külön erre a célra kijelölt szervezet hajtotta végre, de a megszervezése minden esetben

híradó- és informatikai feladat. Az FTP hírhálózat a híradó- és informatikai támogatás egyik eszköze, amely minden tevékenységi fajtában és minden tevékenységi szinten megvalósításra kerül. Az FTP híradás a honi kapcsolattartásnak az egyik eleme, ezért az arra vonatkozó szabályoknak megfelelően kell megszervezni, megtervezni és a menetrendeket kialakítani a távolságok, az út- és terepviszonyok, illetve az esetleges támadások lehetősége alapján.

A kialakított híradó- és informatikai elgondolás alapján a különböző területekhez hozzá kell rendelni a támogatást nyújtó híradó- és informatikai eszközöket. Az előző alfejezetben felvázolt technikai jellemzőkre vonatkozó adatok alapján, és az interoperabilitási képesség teljesítése szerint kell kiválasztani a technikai eszközöket. A legideálisabb, ha a teljes eszközparkunk interoperabilis a többi nemzetével, de főként az elöljáró technikai eszközeivel. Az MH által alkalmazott MRR rádiók megfelelően teljesítik a feladatok támogatását, de nem interoperabilis [15] más nemzetek rádióival, így ezeket csak a saját erőinkkel történő összeköttetések megvalósítására lehet felhasználni. A missziós környezetben szolgálatot teljesítő szakbeosztású állomány által levont következtetések alapján, a HARRIS típusú rádiókészülékek viszont jól alkalmazhatók a többnemzeti környezetben. A terepviszonyok nem minden esetben teszik lehetővé az URH rádiós összeköttetéseket, ezért a technikai eszköz kiválasztásánál a földrajzi tényezőket is figyelembe kell venni. Jól alkalmazható készülék a PRC-117/F típusú, műholdas kommunikációra is alkalmas rádiókészülék, amely megbízható összeköttetést biztosít az átszeldelt terepen is. A válságreagáló műveletek híradó- és informatikai rendszere kialakítása során tehát kiemelten kell kezelni az interoperabilitás kérdését és az összeköttetés megvalósításának feltételrendszerét.

A híradó- és informatikai rendszer megszervezésének folyamatának következő lépésében ki kell dolgozni azokat az okmányrendszereket, amelyek biztosítják a többnemzeti szintű vezetés és irányítást. Az alkalmazott okmányoknak minden esetben meg kell egyezniük a többnemzeti műveletek során elfogadottakkal. Az okmányoknak tartalmazniuk kell a híradó- és informatikai rendszer létesítésével, üzemeltetésével és védelmével foglalkozó részeket a folyamatos és megbízható rendszer biztosítása érdekében. Mindezek mellett minden híradó állomást a rendszeresített okmányokkal fel kell szerelni, és azok vezetését be kell tartatni. A szakmai felkészítés megtervezése folyamán meg kell határozni azokat a részterületeket, amelyek minden, a válságreagáló műveletben résztvevő katonára egyformán érvényes, illetve fel kell építeni a különböző technikai eszközök, berendezések alapján a szakállomány kiképzését. A felkészítésnek tartalmaznia kell minden technikai eszközre vonatkozóan elméleti és gyakorlati képzéseket, egyéni és kötelék feladatok végrehajtását a kezeléstől a hibaelhárításig.

Mindezek alapján a válságreagáló műveletek híradó és informatikai rendszerének megszervezése és megtervezése összetett feladat, amely a tartalmazza a feladatok függvényében a rendszer struktúrájának, a technikai eszközök kiválasztásának és a személyi állomány felkészítésének mozzanatait [16]. Megállapításunk szerint az eljárást a leírtaknak megfelelően kell végrehajtani, folyamatosan ellenőrizve az újonnan megjelenő igényeket, követelményeket.

Az alfejezetet röviden összegezve és értékelve megállapítható, hogy a híradó- és informatikai rendszer megszervezése során a cél, hogy ki kell alakítani a feladatra szabott, szükséges és elégséges, a NATO-elvárásoknak is megfelelő, együttműködésre és expedíciós műveletekre alkalmas rendszert.

Az általános műveleti követelmények determinálását követően és annak megfelelően, az azt támogató, és minden területet kiszolgáló híradó- és informatikai rendszerstruktúrát kell létrehozni, hogy támogassa a vezetés és irányítást a válságreagáló művelet teljes spektrumában.

A híradó- és informatikai rendszer kialakítását elsősorban a hadműveleti igények, a rendszer követelmények és a technikai megvalósítás hármas egysége határozza meg, amelyek egymással szoros és elválaszthatatlan kapcsolatban állnak.

A híradó- és informatikai rendszer megtervezését a feladatrendszer és a kapcsolatok követelményrendszere figyelembevételével kell végrehajtani, valamint a kiszolgálásra alkalmas technikai eszközökkel és felkészített személyi állománnyal kell megvalósítani, üzemeltetni.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A Magyar Honvédség válságreagáló műveleteiben résztvevő erők támogatása sokrétű, szerteágazó szervezési és tervezési munkát igényel. Az MH Összhaderőnemi Doktrína alapján a harci támogatás a harcoló elemek számára nyújtott tűztámogatásból és egyéb műveleti hozzájárulásokból áll, amelynek szerves része a híradás és az informatika. A válságreagáló műveletek minden oldalú biztosítása és támogatása során korszerű technikai eszközökkel felszerelt, minden vezetési szintet támogató és kiszolgáló, a hálózat nyújtotta képességeknek eleget tevő, valamint a NATO követelményeinek megfelelő komplex híradó- és informatikai rendszert kell létrehozni, telepíteni és üzemeltetni.

A korszerű híradó- és informatikai eszközökkel támogatott hadműveleti vezetés biztosítása megtervezésének első fázisa az infokommunikációs rendszer megszervezése, megtervezése. Ennek érdekében meg kell vizsgálni mindazon szabályzókat, eljárásokat, feltételeket, igényeket és követelményeket, amelyek figyelembe vételével kialakítható a vezetés infokommunikációs támogatása. A rögzítettek alapján ennek a szervezési folyamatnak az általános hadműveleti tevékenységekre jellemző eljárásai mellett szükséges megvizsgálni a többnemzeti válságreagáló műveletek sajátosságait is. Az első alfejezetben felsorolt, a híradó- és informatikai rendszerre vonatkozó követelményeket a válságreagáló műveletekben résztvevő erők általános képességeinek megfelelően határoztuk meg. A rögzített követelmények biztosítják, hogy a rendszer megfeleljen azon elvárásoknak, amelyeket a Szövetség támaszt a többnemzeti műveletekben résztvevő erőkkel szemben.

A szervezési folyamat során figyelembe kell venni továbbá azokat az egyéb befolyásoló tényezőket, amelyek szorosan kapcsolódnak a követelményekhez, és meghatározzák a kialakításra kerülő rendszerstruktúrát.

A híradó- és informatikai rendszerrel szemben támasztott követelmények, valamint a megszervezést, megtervezést befolyásoló tényezők alapján kell kialakítani a vezetés és irányítást támogató technikai rendszert. A folyamat a hadműveleti igények, a rendszerkövetelmények és a technikai megvalósítás lehetőségeinek kapcsolatrendszerén alapul, amelyek együttesen, egymásra hatást gyakorolva, kiegészítve biztosítják az alkalmazásra javasolt eljárásmódot.

Összegezve megállapítható, hogy az általános szervezési kérdések mellett a nemzetközi, többnemzeti műveletek során szerzett tapasztalatokat megvizsgálva és elemezve, a meghatározottak felhasználásával egy olyan rendszer kerülhet kialakításra, amely megfelelően képes támogatni mindennemű többnemzeti válságreagáló művelet vezetés és irányítását.

A fejezettel kapcsolatos következtetéseim alapján megállapítható, hogy a vezetés támogatása érdekében biztosítani kell az optimális mennyiségű, minden területre és részfeladatra kiterjedő információkkal történő ellátását, valamint a megszerzett információk feldolgozását, azok továbbítását. Mindezt a többnemzeti műveletek eddigi tapasztalatai is megerősítik.

Az információk feldolgozása és cseréje érdekében meg kell szervezni a komplex, NATO követelményeknek megfelelő, többnemzeti együttműködésre alkalmas, rugalmas, moduláris felépítésű, magas készenléti fokú, és az információk védelmét biztosító korszerű technikai eszközökkel felszerelt híradó- és informatikai rendszert.

A rendszer kialakításánál figyelembe kell venni mindazon tényezőket, amelyek negatív hatást gyakorolhatnak, valamint azokat az összetevőket, amelyek elősegítik a legátfogóbb támogatást nyújtó infokommunikációs rendszer létrehozását.

A válságreagáló műveleteket támogató híradó- és informatikai rendszer megszervezésének folyamatát a hadműveleti igények, a rendszerkövetelmények és a technikai megvalósítás lehetősége alapján kell meghatározni. Ezen hármas tényező minden esetben a folyamatos ellenőrzés és visszacsatolás alapelve szerint jelenik meg a munkasorrend, munkafolyamat során.

FELHASZNÁLT IRODALOM

[1] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás Honvédelmi Minisztérium kiadványa, 2010; p.: 68.

[2] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében (doktori PhD értekezés) Budapest, 2007 p.: 108.

[3] Magyar Sándor: Katonai kommunikációs igények lehetőségek a békefenntartás vezetésének támogatásában (doktori PhD értekezés) Budapest, 2008 p.: 21.

[4] Magyar Sándor: Katonai kommunikációs igények lehetőségek a békefenntartás vezetésének támogatásában (doktori PhD értekezés) Budapest, 2008 p.: 23.

[5] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás Honvédelmi Minisztérium kiadványa, 2010; p.: 23.

[6] Ványa László: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységekre (doktori PhD értekezés) Budapest, 2001 p.: 96.

[7] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás Honvédelmi Minisztérium kiadványa, 2010; p.: 82.

[8] Koronczai Tibor: Missziós híradó-felkészítés az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezrednél, In: Honvédségi Szemle; 64. évf. 1. szám (2010. január); p.: 16. (HU ISSN 2060-1506)

[9] Magyar Sándor: Katonai kommunikációs igények lehetőségek a békefenntartás vezetésének támogatásában (doktori PhD értekezés) Budapest, 2008 p.: 26.

[10] Süle Attila–Csabianszki Viktor: A Magyar Honvédség tapasztalatfeldolgozó rendszeréről, In: Honvédségi Szemle; 62. évf. 1. szám (2008. július); p.: 16. (HU ISSN 2060-1506)

[11] http://www.hm.gov.hu/miniszterium/mh_muvelet_iranyito_kozpont (letöltve: 2009.05.25)

[12] Bene Iván: A Magyar Honvédség tábori híradásának fejlesztése, a fejlesztés 2004. évi időszerű kérdései – 6. dia; MH HVK Híradó és informatikai Csoportfőnökség Elvi Tervező Osztály; Budapest, 2004.

[13] Sándor Miklós–Farkas Tibor–Jobbágy Szabolcs: Híradásszervezés jegyzet a BJKMK híradó tanszék BSc, MSc, és PhD hallgatói számára; ZMNE Budapest, 2009; p.: 13-14.

[14] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal)

[15] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919)

[16] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919)

Farkas Tibor – Pándi Erik – Tóth András
farkas.tibor@zmne.hu – pandi.erik@zmne.hu – toth.hir.andras@zmne.hu

A VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSÁNAK ELMÉLETI ALAPJAI[1]

Absztrakt

Jelen közlemény a Magyar Honvédségben alkalmazott híradó és informatikai támogatás kérdéseit dolgozza fel.

This publication discusses the questions related to Communication and IT support operated at the Hungarian Military.

Kulcsszavak: *Magyar Honvédség, állandó hírrendszer, tábori hírrendszer ~ Hungarian Defence Forces, permanent military network, field military network*

BEVEZETÉS

Az elmúlt évek, évtizedek során a biztonsági környezet folyamatos változáson ment keresztül. A különböző nemzeti- és nemzetközi kutatási eredmények, megállapítások, és a világban végbemenő folyamatok azt mutatják, hogy a viszonylag kisméretű fegyveres összecsapások rendkívül komoly hatást gyakorolhatnak az adott régióra, földrészre, amelynek következményei alól egyre nehezebben vonhatjuk ki magunkat. A háborús és nem háborús műveletek aszimmetrikus hatásai nagymértékben befolyásolják az országok biztonságát, ezért véleményünk szerint e műveletek elemzése napjaink legfontosabb kutatási területévé vált. A nemzetközi színtéren kialakuló konfliktusok nem minden esetben láthatóak előre, de a vallási-, nemzeti- és etnikai ellentétek, területi követelések, gazdasági egyenlőtlenségek és egyéb más összetűzések fennállása esetén nagy valószínűséggel kialakulhatnak, és ennek megelőzésére, megszűntetésére történő nemzetközi fellépés fontos eleme a globális biztonság megteremtésének.

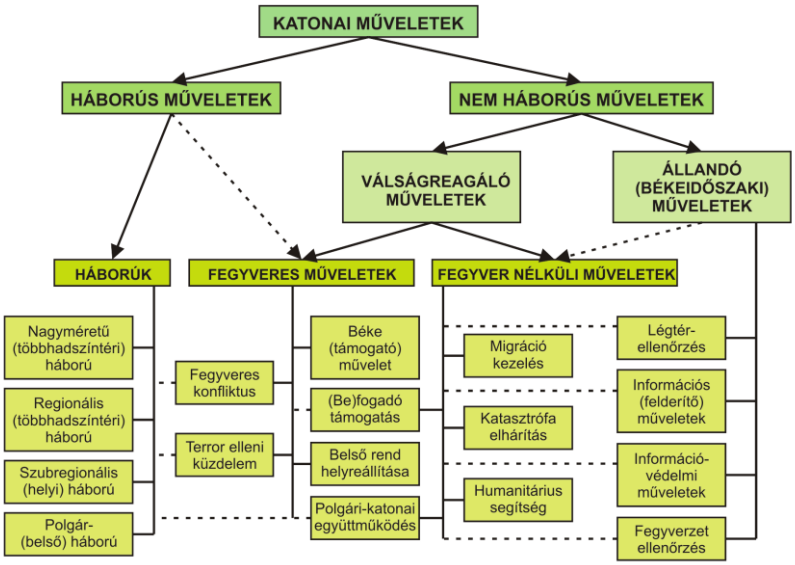
1. FOGALOMTISZTÁZÁS

E témakörben fontosnak tartjuk a kapcsolódó fogalmak tisztázását, amely a későbbiekben alkalmazott terminológiák pontosságát hivatott megalapozni. A válság fogalmát a szakirodalmak, publikációk sokféleképpen határozzák meg, számos definíció fellelhető. A békétől eltérő válsághelyzetre Resperger István doktori értekezésében az alábbi meghatározást alkalmazta: „A válsághelyzet jellemzője, hogy a jó kapcsolat valamilyen vita vagy érdek/érték összeütközés következtében megromlik, feszültség keletkezik a résztvevők között, akik valamilyen eszközzel (politikai, diplomáciai, gazdasági, katonai) megpróbálják a kialakult helyzetet befolyásolni. [1] Véleményünk szerint a válság nemzeti és/vagy nemzetközi helyzet, amelyben a résztvevők és azok valamilyen érdekei fenyegetésnek vannak kitéve, maguk után vonva fegyveres összecsapás, háború kialakulását.

A válságok kezelésére, és azokra történő reagálásra nagy hangsúlyt kell fektetni. A válságkezelést Kőszegvári Tibor a következőképpen fogalmazta meg: „A válságkezelés: politikai reagálások modulálása ingatag helyzetben; a saját érdek érték képviselete

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

érdekében. Ne kényszerítse az ellenfelet akció- reakció végrehajtására. Számos tekintetben jó politikai és diplomáciai lépések sorozata." [2]. A katonai műveletek osztályozása során látható, hogy a válságreagáló műveletek a nem háborús katonai műveletek körébe tartoznak, melyeknek rendszerét Deák János az alábbi ábrával szemlélteti publikációjában.



1. ábra: A katonai műveletek típusai
Forrás: [3]

A katonai műveletek osztályozásának egyik lehetséges változata szerint a válságreagáló műveletek a nem háborús katonai műveletek csoportjába tartoznak, amelyek fegyveres- és fegyver nélküli beavatkozást eredményezhetnek. A nem háborús műveletek csoportjába sorolják a mértékadó szakirodalmak a béketámogató- és a humanitárius műveleteket, a kutató-mentő feladatokat, a terrorizmus elleni küzdelmet, a légtérellenőrzést, az információs műveleteket. Az ábrán jól látható, hogy a háborús- és nem háborús műveletek közötti határvonalon elhelyezkedő, napjainkban kiemelt fontossággal bíró válságreagáló műveletek hordozhatják mindkét típus jellemzőit. A Magyar Honvédség Összhaderőnemi Doktrína 3. kiadása (MH ÖHD) alapján a műveletek két kategóriába sorolhatóak, amelyek az 5. cikk szerinti kollektív védelem műveletei, és a nem 5. cikk szerinti válságreagáló műveletek. [4] Kutatásainknak megfelelően, a következő alfejezetben a NATO válságreagáló műveleteinek alapelveit, osztályozását kívánjuk megvizsgálni.

2. A NATO VÁLSÁGREAGÁLÓ MŰVELETÉNEK ALAPELVEI, A SZÖVETSÉGES ERŐK KÉPESSÉGEI

A nem háborús katonai műveletek (MOOTW: Military Operations Other Than War) új típusú sajátos szemléletet, és az adott válság rendezéséhez legalkalmasabb, változó összetételű szervezeteket követeltek meg. A politikai döntéseket követően, a megalakításra kerülő katonai szervezeteket különböző civil egységekkel kooperálva szervezik meg, amelyek együttműködése a sikeres műveleti feladat végrehajtásának alapvető követelménye. A létrehozott ideiglenes katonai szervezetek speciális kiképzési, felkészítési formákat

igényelnek az adott területnek megfelelően, és a végrehajtott műveletek megkövetelik az egyéni-, technikai biztosítást, felszerelést és a szilárd, rugalmas vezetést[2].

A NATO válságreagáló műveleteknek (CRO: Crisis Response Operations) nevezi azokat a tevékenységeket, amelyek a kialakult konfliktus kezelésére, esetlegesen megelőzésére, a válságkezelésre irányulnak. Tehát a CRO minden esetben egy összetett, többfunkciós művelet, amely során katonai képességek kerülnek felhasználásra polgári-, humanitárius- és más rendészeti szervekkel együttműködve, és amely a megelőzésre, ellentevékenységekre, a kialakult helyzet stabilizálására, esetlegesen egyéb kiegészítő tevékenységekre irányul. Természetesen ezeknek a műveleteknek összhangban kell lenniük a vonatkozó nemzetközi jogokkal, felhatalmazásokkal és mandátumokkal. Az 1999-ben elfogadott stratégiai koncepció (Washington, 1999. április 23.) alapján a Szövetség legfontosabb feladata a különböző konfliktusok, az instabil államok helyzetéből adódó biztonsági kockázatok megszüntetése és felszámolása, kiemelve a közel-keleti és észak-afrikai térség biztonsági kockázatát. Véleményünk szerint ezt a dokumentumot kell tekinteni az alapvető, a jelenleg is érvényben lévő elvek „alapkövének". A NATO Katonai Bizottsága (Military Committee) segíti a Szövetséget az átfogó stratégiai koncepciók kidolgozásában az általuk elkészített dokumentumokkal (MC), amelyek ajánlások a katonai erők felkészítésre és a készenléti tervek végrehajtására. Ebben az időszakban kerültek felállításra a többnemzeti összhaderőnemi alkalmi harci kötelékek (CJTF: Combined Joint Task Forces), amelyek rugalmas, mozgékony kötelékek a többfunkciós alkalmazások ellátására.

A NATO-t létrehozó Észak-atlanti Szerződés 14 cikkelyből áll, amely V. cikkelye rendelkezik a kollektív védelemről. Az V. cikkely értelmében bármely tagállamot ért támadás az egész Szövetség elleni támadást jelenti, amellyel szemben a szervezet fegyveres fellépést tesz a béke és biztonság helyreállítása érdekében. Az idő előrehaladtával, a technológiai fejlesztések rohamos ütemével párhuzamosan megváltoznak a veszélyek jellegei, ezért napjainkban a szakértőkben több kérdés is felmerül, amelyek alapjaiban változtatják meg az alapelveket, stratégiákat. Ilyen a kibernetikai támadások kérdésköre is. Rábai Zsolt előadásában felhívta a figyelmet, hogy egy NATO-tagország elleni hagyományos értelemben vett támadásra történő reagálást tartalmazza az V. cikkely, de ha az adott nemzet gazdaságát is fenyegető számítógépes támadás éri a tagállamot, akkor felmerül a kérdés, hogy az értelmezhető vagy sem az V. cikkelyben megfogalmazottak szerint. [5] Az előzőekben leírt válságreagáló műveletek a NATO válságkezelésének részét képezi, amelyet az V. cikkely alá nem tartozó műveletekként azonosítja a Szövetség.

A NATO alapokmányai közül meg kell említenünk az 5. Cikkelyen Kívüli Válságreagáló Műveletek Doktrínát (AJP-3.4 Non Article 5, Crisis Response Operations; NATO, 2005. március 1), a Katonai Tanács dokumentumát az MC 327/2-t (NATO Military Policy for Crisis Response Operations)[3] és a Szövetséges Összhaderőnemi Doktrínát (AJP-01C, NATO 2006). A dokumentumok és a koncepció szerint fel kell készíteni a tagállamok fegyveres erőit a válságok kezelésére, fegyveres konfliktusokra, melyek célja, hogy a Szövetség kellő időben és összehangoltan reagáljon a fenyegetésekre. A szabályzatok, okmányok minden esetben behatárolják a vezetés és irányítást, a részvételt a műveletek teljes spektrumában és a különböző típusú műveleteket. A tagországok az ilyen típusú műveletekben nem minden esetben vesznek részt, eltérően a kollektív védelemtől. A Szövetség esetleges felkérésére, a nemzetek politikai döntését követően vállalnak feladatokat lehetőségeikhez mérten. A megszervezésre kerülő többnemzeti műveletek két fő kategóriákba sorolhatók, amelyek a béketámogató műveletek (Peace Support Operations) és az egyéb műveletek.

A különböző nemzeteket, szervezeteket figyelembe véve ez az alapvető felosztás eltérő lehet, amelyet az alábbiakban fogalmaztak meg a szerzők „A Válságreagáló műveletek elmélete és gyakorlata a 21. században" című egyetemi jegyzetben: „Mindenek előtt célszerű

2 A speciális felszerelés, technikai biztosítás természetesen a híradó- és informatikai rendszereket is magába foglalja, amelyek alkalmazása kiemelt fontosságú a vezetés és irányítás támogatásában

3 Irányadó a CRO műveletek tervezéséhez szervezéséhez és meghatározza a vonatkozó alapelveket, szempontokat

tisztázni, hogy mint minden felosztás ez is esetleges. A válságreagáló műveletek meghatározására az egyes országok, a NATO, és más nemzetközi szervezetek által elfogadott és használt felosztás nem egységes. A NATO-ban használt felosztás szerint ezek az alábbiak: Először béketámogató műveletek […] Másodszor, Humanitárius műveletek […] Harmadszor, Kutató-mentő műveletek. [6]

A béketámogató műveletek valamilyen nemzetközi szervezet (Egyesült Nemzetek Szervezete: ENSZ, Európai Biztonsági és Együttműködési Szervezet: EBESZ) felhatalmazását követően kerülnek végrehajtásra a Szövetség vezetésével, a feladatokat ellátó nemzetek részvételével. Fontos megjegyezni, hogy ezekben a műveletekben a nem NATO tagállamok is részt vehetnek, felajánlhatnak erőket. A béketámogató műveletek az alábbiak szerint lehet szétválasztani, a konfliktushelyzet kialakulásától kezdve a békeállapot újbóli eléréséig, időrendben. (Természetesen ezek szintén változhatnak a válság intenzitásától, a közbelépéstől, és egyéb más tényezőtől.)

A konfliktus megelőzés (conflict prevention) a diplomáciai lépésektől általában a kijelölt alegységek telepítéséig terjedő időszak tevékenységei, melyek magukba foglalják a fegyveres összetűzések kialakulásának megakadályozását.

A béketeremtés (peace-making) a konfliktus megelőzést követő tevékenység, amely a már kirobbant fegyveres összetűzések megfékezésére irányul, főként diplomáciai úton és megelőző katonai lépésekkel.

A békekikényszerítés (peace enforcement) olyan diplomáciai, katonai, gazdasági lépések (vagy együttes alkalmazása) adaptálása, amelyet a békés eszközök eredménytelenségét követően katonai kényszerítő eljárásmód követ.

A békefenntartás (peace-keeping) célja, hogy a már kialakult (kikényszerített) béke helyzetet a műveletekben résztvevő erők stabilizálják, fenntartsák, az esetleges ellentéteket enyhítsék valamennyi fél hozzájárulásával.

A békeépítés (peace building) azon eljárások összessége, amelyek megszűntetik a kialakult konfliktusok okait, és elősegítik a konfliktus előtti állapotok visszaállítását, de a feladatok végrehajtása során már a polgári szervezetek tevékenységén van a nagyobb hangsúly, akik tovább erősítik a lakosság életének visszaállítását, a gazdaság újbóli fellendülését.

A humanitárius segítségnyújtás/műveletek (humanitarian relief) azon tevékenységek összessége, amelyek az emberek életének elősegítését biztosítják, többnyire civil szervezetek végrehajtásával és esetleges katonai biztosítással.

A válságreagáló műveletek másik csoportjába tartoznak a különböző feladat végrehajtások támogatására irányuló tevékenységek, amelyek nemzeti vagy többnemzeti szinten egyeztetett feladatok. Ezek lehetnek:

- humanitárius segítségnyújtás támogatása;
- kutató-mentő feladatok ellátása, biztosítása;
- a civil szervezetek és hatóságok katonai támogatása;
- esetleges evakuálási, kiürítési feladatok végrehajtása, biztosítása;
- katasztrófák megszüntetésében való részvétel.

Ezeket a feladatokat és azok sikeres végrehajtását nagymértékben befolyásolja a résztvevő állomány összetétele (katonai, civil, egyéb hatóságok, más fegyveres szervezetek, kormányzati-, és nem kormányzati szervek), az adott terület mérete és földrajzi elhelyezkedése, a tevékenységet folytató erők nemzeti összetétele, és természetesen a politikai döntések és jogi szabályozások. A válságreagáló feladatok tehát olyan tevékenységek összessége, amelyek az adott ország, régió béke állapotát megszüntető konfliktushelyzetet (esetlegesen háborút), vagy a területen kialakult egyéb válságokat felszámolja az újbóli béke megteremtése érdekében. Az előzőekből jól látható, hogy a tevékenységek jelentős részében a katonai jelenlét elkerülhetetlen, így a nemzeti haderők

képességei meg kell, hogy feleljenek a hagyományos értelemben vett háborús feladatok mellett az ilyen típusú műveletek ellátására.

3. A KÉPESSÉGEKET BIZTOSÍTÓ NEMZETI FEJLESZTÉSI IRÁNYOK

A NATO által vezetett válságreagáló műveletekben résztvevő nemzetek haderői a feladatok sikeres végrehajtása érdekében a korszerű technikai követelményeknek, vezetés és irányítási elveknek, és a magas fokú együttműködő képességnek kell, hogy megfeleljenek. A nemzetek tapasztalatainak megfelelően, és a műveletek sajátosságait figyelembe véve kell meghatározni az irányelveket a nemzeti fejlesztések során. Első megközelítésben a feladat végrehajtást befolyásoló és a képességeket meghatározó alapvető tényezők az alábbiak:

- a válságreagáló művelet típusa, jellege;
- a küldetés várható időtartama;
- a misszió során végrehajtásra kerülő feladatok;
- az előzőből következik a végrehajtó erők összetétele;
- amely a feladatok mellett meghatározza az egyéb, nem katonai erők, szervezetek jelenlétét;
- a műveleti terület kiterjedése, amely megszabja a résztvevő erők méretét;
- a műveleti terület földrajzi helye, amely a logisztikai biztosítást is nagymértékben befolyásolja;
- a szélsőséges időjárási és környezeti tényezők jelenléte;
- a feladatokból eredően a felhasználásra kerülő mindennemű technikai eszközöket és fegyverzetet;
- speciális képességek, amelyek a siker kivívásának alapfeltételei.

A felsorolt tényezők nagymértékben meghatározzák a megszervezésre, megtervezésre kerülő híradó- és informatikai rendszert, amely képes támogatni az erők feladatának végrehajtását. A nemzetközi- és hazai missziós tapasztalatok alátámasztják, hogy a jelen konfliktusai, válságai szövetséges rendezéséhez nem tömeghadsereg alkalmazására van szükség, hanem kisebb méretű, többfunkciós képességekkel rendelkező, korszerű haditechnikai eszközökkel felszerelt katonai erőkre (civil szervezetek támogatásával), amelyek a jellegükből adódóan képesek a konfliktusok felszámolására a nemzetközi béke helyreállítása érdekében. Fontos megjegyezni, hogy a nagyfokú mozgékonyság és az „önellátó” képesség egyik alapvető követelménye a katonai erőknek, számítva a felügyelt terület nagyságra és a távoli országokban történő alkalmazásra. Ezeket figyelembe véve a hagyományos katonai szervezetekhez hasonlóan, vezető-, végrehajtó-, támogató alegységeknek, részlegeknek egyaránt jelen kell lenniük a szervezetekben. Alapvetően a műveletek speciális jellegéből adódóan főként könnyűfegyverzettel és könnyű páncélozott szállító járművekkel kell ellátni az alegységeket, amelyek a saját erők megóvását képesek biztosítani. Természetesen ezek is változnak a feladatok függvényében, és az ellenséges erők és fegyveres fenyegetések intenzitásának mértékétől.[4]

A nemzeti védelmi képességek fejlesztésének minden területen jelen kell lennie a mozgékonyság/mobilitás és a csapataink megóvása (Force Protection) érdekében, amelyek összhangban vannak a Szövetség által támasztott követelményekkel. A magyar védelmi képességek fejlesztése két részre osztható a feladatok alkalmazása tükrében, melyek a következők: MH nemzeti feladatok végrehajtását előmozdító fejlesztések; a NATO feladatrendszerével összefüggő fejlesztések. A két terület eltérést mutathat, de a folyamatnak figyelembe kell vennie a Nemzeti Katonai Stratégiában[5], az MH Összhaderőnemi

4 A humanitárius feladatok ellátása során a képességek főként a végrehajtására (pl.: szállítás) összpontosulnak, de a fegyverzeti és technikai összetevők a fenyegetettséghez igazíthatók. (pl.: MH Iraki Szállító Zászlóalj)
5 1009/2009. (I. 30.) Kormány határozat a Magyar Köztársaság Nemzeti Katonai Stratégájáról

Doktrínában és egyéb vonatkozó nemzeti- és szövetséges dokumentumokban meghatározottakat, amelyeket ki kell egészíteni a nemzetközi szerepvállalás során szerzett tapasztalatokkal.

A képességek kialakítása során a jövőbeni műveletekben való részvételekkel is számolni kell, amelyek az eddigiektől eltérőek, magasabb intenzitásúak is lehetnek, ezáltal megváltoztathatják a fejlesztési koncepció főbb irányvonalait. Véleményünk szerint a nemzetközi helyzet, a szövetség követelményei alapján két irány közül kell választani a fejlesztések területén az MH vonatkozásában, amelynél minden esetben figyelembe kell venni a nemzetközi műveletekben való részvételünket:

- Olyan többfunkciós haderő felállítása, amely folyamatosan, a kor követelményeinek megfelelően, és az elvárásokhoz igazítva fejleszthető. Az ilyen haderő általános alkalmazásra használható fel, amely a moduláris felépítéséből adódóan gazdaságosan és jól alkalmazható;
- Speciális feladatokat ellátó erők felállítása, amely nem, vagy csak igen drágán fejleszthető, de az adott tevékenységre legjobban felhasználható.

Megítélésünk szerint csak az olyan haderő „életképes” napjainkban és a jövőben, amely többcélú, gyorsan bevethető, mozgékony, a magas és alacsony intenzitású fegyveres konfliktusokban sikereket elérni képes, kisebb anyagi ráfordítással fejleszthető, a moduláris felépítéséből adódóan feladatorientált képességekkel bíró és megfelelő vezetés és irányítással támogatott. (A prágai-csúcson elhangzottak alapján a NATO tagállamok hadseregeinek részfeladatokra kell specializálódniuk.) Mindezek mellett kiemelten kell kezelni a haderő (és a műveletekben résztvevő „kontingensek”) híradó és informatikai támogatását, amely nélkül nem valósulhat meg a csapatok vezetése és a korszerű fegyverek irányítása.

A jelenlegi válságreagáló műveleteket megvizsgálva látható, hogy túlnyomórészt a Szövetség területétől távoli helyeken kialakuló konfliktusok és válságok megszüntetésére került sor. Ennek értelmében a már említett, a külföldön bevethető erők képességét fontosnak tartjuk röviden megvizsgálni. Ez a NATO megfogalmazásában az expedíciós képesség (expeditionary capabilities). Amellett, hogy megvalósul a nemzeti kijelölt erő „kitelepítése” a műveleti területre, további képességek birtokában kell lennie az ottani műveletek ellátásához. A fellelhető publikációk közül ezt a témakört részletesen taglalja Sticz László és Csák Zoltán, akik szerint:

„Megállapítható, hogy egy adott expedíció két fő részre bontható:

Az expedíciós erő kiválasztása, összeállítása, felkészítése és bevetése az adott területre, és az adott feladat végrehajtása, valamint,

Az erők folyamatos, magas színvonalú hazai bázisról történő támogatása. Az expedíciós műveletek végrehajtása, egy olyan erős támogatási rendszer kiépítését követeli meg, amely minden körülmények között képes a feladat hathatós támogatására a misszió befejezéséig és a csapatok hazatelepítéséig. Következtetésképpen megállapíthatjuk, hogy a logisztikai támogatás, a felkészítés, a telepítés, az alkalmazás, és a műveletek fenntartása egy központi, igen fontos része az expedíciós műveleteknek.” [7]

Tehát az expedíciós képesség tágabb értelemben az adott nemzet határain kívüli műveletekben való „önfenntartó” részvételt jelent, amely biztosítja az erők feladat-végrehajtásának mindenoldalú támogatását és lehetőségeit, beleértve a mobilitást, a túlélő képességet, rugalmasságot. A 2002-ben elindult védelmi felülvizsgálat a képességeket és kihívásokat figyelembe véve meghatározta a főbb fejlesztési irányokat. Az eljárás végeredményeként megállapították, hogy egy rugalmasan alkalmazható, szövetséges és nemzeti feladatok ellátására egyaránt alkalmas, széleskörű tevékenységeket végrehajtani képes, könnyű fegyverzettel ellátott mobil és telepíthető szárazföldi erőre van szükség, amely képes többnemzeti együttműködésre.

A Magyar Honvédség fejlesztései irányának tehát minden esetben arra kell törekednie, hogy megfeleljen mind az országvédelem, mind a nemzetközi szerepvállalás követelményeinek. A fejlesztés nem kizárólag a haditechnikai eszközökre kell, hogy irányuljon, hanem a személyi állomány kiképzésére, felkészítésére, és a vezetési rendszerre egyaránt. Az Országgyűlés 51/2007-es határozatában a következőket fogalmazta meg a további fejlesztések irányairól: „Az Országgyűlés szükségesnek tartja a Magyar Honvédség fejlesztésének folytatását. Ennek során a fő hangsúlyt a nemzeti és nemzetközi keretek közötti alkalmazás követelményeinek egyaránt megfelelő katonai képességek kialakítására kell helyezni. […] jöjjön létre egy professzionális, sokoldalúan, rugalmasan és hatékonyan alkalmazható, nemzetközi (NATO, EU, ENSZ, EBESZ) együttműködésre képes, kiképzett, feltöltött és bevethető szervezetekkel rendelkező, korszerű eszközökkel felszerelt és finanszírozható haderő. […] A fejlesztési feladatok fontossági sorrendjét a Magyar Honvédség professzionális, valamint a műveleti területre telepíthető, ott együttműködésre és működőképességének fenntartására alkalmas (expedíciós) jellegének erősítése határozza meg. […] a feladatok ellátására alkalmas, költségtakarékosan működtethető haderőt kell kialakítani és fenntartani;" [8]

A komplex és gyorsan változó biztonsági környezetnek megfelelően, a szervezeti és képességbeli átalakítás folytonossága a sikeres válságreagáló műveletek végrehajtásának alapköve. Sajnálatos, hogy a NATO tagállamok fejlesztési ütemét nagymértékben lelassította a 2008-2009-es gazdasági válság. A finanszírozási kérdésekben jelentős problémák jelentek meg, amelyek nem csak a fejlesztésekre gyakoroltak negatív hatást, de a missziós feladatok ellátásának pénzügyi támogatását is jelentősen megnehezítették. Ennek tükrében merült fel annak lehetősége, hogy a megelőző diplomáciára és a válságterületek nemzeti haderőinek kiképzésére kell nagyobb hangsúlyt fektetni, amely kevesebb költséggel jár. További megoldást jelenthet a közös beszerzések végrehajtása is, amely a többnemzeti műveletekhez hasonlóan csökkentheti a NATO tagállamok költségeit.[6] Szenes Zoltán előadásában kihangsúlyozta, hogy a multinacionális finanszírozás a fejlesztések és feladatellátások során az egyetlen lehetőség a Szövetség számára, amely biztosítja a NATO jövőbeni sikeres feladatellátásának alapjait. [9]

4. A MAGYAR HONVÉDSÉG LEHETSÉGES NEMZETKÖZI FELADATAI, A HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁS DEFINÍCIÓJA

A Magyar Köztársaság NATO műveletekben való részvétele – várhatóan – a jövőben is meghatározó lesz. Az előző alfejezetben leírtaknak megfelelően, az Észak-atlanti Szerződés V. cikkely és a nem V. cikkely szerinti műveletekben való részvétel alapvető kritériuma a képességeknek, kihívásoknak való megfelelés. Az ország biztonságát fenyegető globális, regionális és közvetlen környezetből származó fenyegetések nagymértékben befolyásolják a stratégiánkat. A Magyar Köztársaság Nemzeti Katonai Stratégiájában megfogalmazottak szerint a honvédelem két pillére a nemzeti önerő és a szövetségi együttműködés. Az MH feladatai e két területnek megfelelően tevődik össze, az előzőekben tárgyalt képességekhez és fejlesztésekhez hasonlóan. A magyar katonai erők külföldi alkalmazására minden esetben nemzetközi felhatalmazást követően kerülhet sor, amelyet jól tükröz az eddigi missziós tevékenységünk is. Az MH nemzetközi műveletekben való részvétele mindenkor valamilyen együttműködés keretén belül valósul meg, amellyel közvetve vagy közvetlenül szavatolja az országunk és a Szövetség védelmét. A Magyar Köztársaság nemzeti biztonsági stratégiája[7] felsorolja azokat a kihívásokat, amelyek meghatározzák a feladatokat a biztonság megteremtése, megóvása érdekében. [10] A legfontosabb kihívásoknak a tárgyalt témához kapcsolódóan az úgynevezett globális kihívásokat tartjuk, amely csoportjába a terrorizmus, a

6 Tíz NATO nemzet és két Partnerség a Békéért (PfP: Partnership for Peace) programban résztvevő ország közreműködésével valósult meg a Stratégiai Légi Szállítási Képesség (SAC: Strategic Airlift Capability)
7 2073/2004 . (IV. 15.) Kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

tömegpusztító fegyverek elterjedése, az instabil régiók veszélyei, az illegális migráció, a gazdasági instabilitás, az információs társadalom kihívásai és a globális természeti- és civilizációs veszélyforrások állnak. Ezek megakadályozása és elterjedése érdekében mind a Szövetség, mind az ország olyan haderőt tart fenn, amely többnemzeti együttműködésben, hagyományos és aszimmetrikus hadviselés kereti között képes reagálni a kialakult helyzetre. A következőkben meg kell vizsgálni a Magyar Honvédség lehetséges feladatait, amely alapdokumentuma a már említett Magyar Köztársaság nemzeti katonai stratégiája és a Magyar Honvédség Összhaderőnemi Doktrínája.

5. A MAGYAR HONVÉDSÉG FELADATRENDSZERE A TÖBBNEMZETI MŰVELETEKNEK MEGFELELŐEN

A Magyar Honvédség alaprendeltetése az ország szuverenitásának és területének védelme. A NATO-hoz történő csatlakozásunkat követően – szövetségi megközelítésben – mindez a szövetség keretein belül valósul meg, az Észak-atlanti Szerződésben foglalt kollektív védelem értelmében. Természetesen a segítséget nyújtó szövetséges erők megérkezéséig a Magyar Honvédségnek képesnek kell lennie az önálló védelmi feladatok végrehajtására. Ennek megfelelően a légtérvédelem biztosítására kiemelt hangsúlyt kell fektetni, amely a NATO integrált légvédelmi rendszerének (NATINADS: NATO Integrated Air Defence Systems) támogatásában is megnyilvánul. A NATINADS egy olyan integrált rendszer, amely a Szövetség területének biztonságát szavatolja úgy, hogy felderíti, azonosítja, követi a légtérben megjelenő eszközöket, és szükség esetén megsemmisíti azokat.

Az V. cikkely szerinti műveletek mellett a NATO, így a Magyar Köztársaság is nagy hangsúlyt fektet az eddig tárgyalt válságreagáló műveletekben való részvételre, amely hozzájárul a nemzetközi béke és biztonság megteremtéséhez. A vállalt kötelezettségeknek megfelelően a Magyar Honvédség részt vesz különböző nemzetközi műveletekben, hozzájárulva a szövetséges küldetések ellátásához az arra kijelölt és felkészített katonai erők felajánlásával, amely nagymértékben elősegíti a terrorizmus elleni harc katonai feladatainak ellátását.

A Magyar Honvédség hadműveleti magasabb egysége, mint középszintű irányító-vezető szerve, az MH Összhaderőnemi Parancsnokság. Feladatait a HM Honvéd Vezérkar Főnök közvetlen irányítása alá tartozó szervezetekkel, a rendvédelmi szervekkel, a katasztrófavédelem erőivel, és a szövetséges erőkkel együttműködve hajtja végre.

A válságreagáló műveletek feladatait ellátni képes korszerű, a kor kihívásainak eleget tevő haderő megteremtése kizárólag a követelmények meghatározásával, a fejlesztések és felkészítések végrehajtásával valósítható meg, a feladatok folyamatos bővülésének nyomon követésével. Természetesen a feladatok határozzák meg a haderőfejlesztés irányát, de a fejlett technikai eszközökkel felszerelt és kiképzett katonai erők is meghatározzák azt, hogy milyen műveleteket képes ellátni. A már említett MH képességi ambíció szintje[8] behatárolja a további kutatási és fejlesztési feladatok irányát. A végrehajtott többnemzeti műveletekben szerzett tapasztalatokat, és a feladatok meghatározását figyelembe véve a legjelentősebb kötelékek a zászlóalj szintű erők, amelyek korszerű technikai eszközökkel és vezetéssel képesek: felügyelni nagyobb területeket, járőrözéseket végrehajtani, megfigyeléseket végezni, ellenőrzési pontokat „üzemeltetni”, információszerzési-, felderítési akciókat végrehajtani, és egyéb nem katonai jellegű feladatok katonai biztosítását ellátni.

A tapasztalatokból és a szakértők kutatási eredményeiből jól látható, hogy tágabb értelemben véve a fenyegetések és az azokat megszüntető feladatok, két fő tevékenység köré összpontosulnak, amelyek a következők: aszimmetrikus fenyegetésekre történő reagálás, hadászati szintű tömegpusztító fegyverek elterjedése és annak megakadályozása. A

8 Az ország határain kívül folytatott műveletekben egyidejűleg egy dandár méretű erő hat havi harci és egy zászlóalj méretű erő tartós (hat hónapon túli) nem harci körülmények közötti alkalmazására; vagy egy zászlóalj méretű erő tartós (hat hónapon túli) harci és egy zászlóalj méretű erő tartós (hat hónapon túli) nem harci jellegű tevékenységére.

többnemzeti műveletek mindkét tevékenységet felölelheti, ezért átfogó feladatellátásra alkalmas, moduláris felépítésű erők alkalmazása a mértékadó. A multinacionális missziók feladatai igen széleskörűek, amelyekben a Magyar Honvédség alegységei csak korlátozott létszámmal, speciális szakterületek ellátását képes felvállalni.

A válságreagáló műveletek széles skálájának minden területén nem képes helytállni a Magyar Honvédség, ezért szövetségi felajánlásokra csak a képességek meghatározását követően kerülhet sor. A korábban már ismertetett CRO feladatok pontosabb meghatározása alapján figyelembe kell venni a kialakult konfliktus intenzitását és annak kiterjedését. A katonai feladatok, amelyekben az MH alegységei részt vehetnek, a konfliktus kezdeti szakaszától a konfliktus felszámolásán keresztül egészen az újjáépítésig tarthatnak. Ezért a tevékenységek az embargók és szankciók bevezetésétől, a hagyományos értelemben vett hadműveletekig terjedhetnek, majd a nem háborús, de fokozott ellenséges tevékenységek jelenléte melletti újjáépítési feladatokig, civil szervek támogatásáig. Az MH ÖHD a következő műveleteket és tevékenységeket sorolja az egyéb, nem V. cikkely szerinti válságreagáló műveletek és feladatok közé:

- humanitárius segítségnyújtás támogatása;
- katasztrófa-elhárítás támogatása;
- kutatás és mentés;
- nem harcolók kimenekítésének támogatása;
- kivonási műveletek;
- katonai segítség/támogatás a civil hatóságok részére;
- szankciók és embargók alkalmazása.

Az eltérő típusokból arra a következtetésre jutottunk, hogy a műveleti feladatokra létrehozott és felkészített alegységek széleskörű alkalmazása igen fontos, ezért különös figyelmet kell fordítani a kontingensek „összeállítása”, megszervezése során a képességekre, kihívásokra. A parancsnok vezetés és irányítása érdekében a híradó és informatikai támogatás elengedhetetlen. A hagyományos híradó és informatikai eszközök, amelyek még igen nagy számban állnak a honvédség rendszerében, nem minden esetben alkalmasak a megújult igények és a parancsnok elvárásainak teljesítésére. Leszögezhető, hogy a hagyományos értelemben vett hadműveletekhez hasonlóan, a válságreagáló műveletek híradó és informatikai támogatása nélkülözhetetlen a tevékenységek sikeres végrehajtása során.

6. A VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSÁNAK FOGALMA, CÉLJA ÉS HELYE A KATONAI MŰVELETEKBEN

Az előző alfejezetben rögzítettek alapján megállapítható, hogy a többnemzeti műveletek keretein belül végrehajtásra kerülő válságreagáló műveletek híradó és informatikai támogatása kiemelt szerepet kell, hogy betöltsön a kijelölt, megszervezett és létrehozott erők kiképzésében, felkészítésében, technikai eszközökkel való ellátásában és a feladat végrehajtásban egyaránt. Minden művelet parancsnoki vezetése érdekében létrehozott, telepített és üzemeltetett híradó- és informatikai rendszernek alkalmasnak kell lennie a meghatározott feladat ellátásának támogatására az információk továbbítása céljából. A folyamatos információcsere a csapatok vezetésének egyik alapvető és legfontosabb tényezője, amely időszakos kiesése is elkerülhetetlenül zavart okozhat. A folyamatos és megbízható összeköttetés nélkül az alegységek vezetése és irányítása nem lehetséges. Az alárendeltekkel, az elöljárókkal és együttműködőkkel való szoros kapcsolattartás megköveteli a híradó- és informatikai erők és eszközök hozzáértő felhasználását. Megbízható híradás nélkül a parancsnokok és törzsek nem képesek az alárendelteket vezetni,

erőkifejtésüket a feladat végrehajtására irányítani. A kommunikáció biztosítása érdekében a szakállomány részére minden esetben meg kell határozni a pontos feladatokat, és részletes tervet kell készíteni, amely a változásokat rugalmasan kezelni. Ezek a megállapítások különösen igazak a missziós feladatok ellátására létrehozott erők vezetése esetén, amely több problémát, például szervezési nehézséget is felvet a kialakításra kerülő kommunikációs rendszer telepítése és üzemeltetése során.

A vezetés és irányítás megfelelő, minden oldalú támogatása nélkülözhetetlen a siker kivívásában. A vezetés és irányítást (C2: Command and Control) az alábbiak szerint fogalmazza meg az MH Összhaderőnemi Doktrína : „Vezetés és irányítás egymással szoros kapcsolatban lévő, de nem szinonim fogalmak. A vezetés jogi kategória, melynek gyakorlása egyszemélyi felelősséghez kötött. Az irányítás a parancsnok által gyakorolt jogkör, amely az alárendeltre átruházható. Ebben az esetben a parancsnok az irányítás kérdéseibe nem avatkozhat bele. A vezetés és irányítás rendszerét a parancsnok és a törzs alkalmazza a hadműveletek előkészítése és végrehajtása során.” [11]

A C2-nek megfelelően a mindenkori parancsnok, mint egyszemélyi vezető, és törzse részére olyan támogatást kell rendelkezésre bocsátani, amely minden esetben biztosítja a vezetés és irányítást. A híradó és informatikai támogatás a parancsnok vezetés és irányításának olyan támogatása, amely biztosítja az alárendeltek vezetését annak folytonosságának fenntartásával. Az előző alfejezetben leírt lehetséges feladatok alapján meg kell határozni a nem háborús katonai műveletek válságreagáló műveleteinek híradó- és informatikai támogatását, mint tevékenységet. Ezek, és a katonai műveletek típusai alapján a nem háborús katonai műveletek híradása magába foglalja [12]:

- a béketámogató műveletek híradó és informatikai támogatását;
- egyéb humanitárius műveleteknek, katasztrófák felszámolásának, kutató-mentő feladatoknak, befogadó nemzeti támogatásnak híradó- és informatikai támogatását;
- információs-, információ védelmi-, légtér-ellenőrzési műveletek híradó és informatikai támogatását.

A nem háborús katonai műveletek híradó- és informatikai támogatása tartalmazza mindazon híradó és informatikai erőket és eszközöket, amelyek békeidőszakban és az esetleges válságok kezelése során alkalmazásra kerülnek.

A híradás és az informatika összefonódása, konvergenciája elkerülhetetlen és szükséges a korszerű csapatvezetés megvalósítása, a növekvő igények teljesítése érdekében. A híradás, mint a csapatvezetés alapvető eszköze az információk továbbításának biztosítására mára már nem teljes körű értelmezést ad a jelenlegi híradó és informatikai támogatásnak. A katonai informatika egyes megfogalmazások szerint a fegyveres erők eredményes működését biztosító informatikai rendszerek összessége.

A parancsnok a vezetés és irányítás támogatásának érdekében híradó- és informatikai rendszer kerül megszervezésre, telepítésre és üzemeltetésre. A C2CS tehát, a vezetés és irányítási kommunikációs (híradó) rendszer, amely a vezetés és irányításhoz szükséges információáramlást biztosítja. A rögzítettek alapján konstatálható, hogy a NATO-ban alkalmazott kifejezések közel azonos irányelveket mutatnak, de minden kifejezés az adott szakterületre vonatkozóan ad szűkebb értelmezést. Természetesen a szakirodalmak és más fejlett NATO hadseregek szakértői további megfogalmazásokat használnak a különböző képességű, de a híradó rendszereken alapuló rendszerek meghatározására. Ilyen a „vezetés, irányítás, kommunikáció, informatika, hírszerzés, megfigyelés, és felderítés” (C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) kifejezés, amelyek sokkal specializáltabb, összetettebb technikai eszközöket és eljárásokat csoportosítanak az adott feladat végrehajtásának támogatása céljából. A fent leírtak alapján fontos kiemelnünk, hogy ezek a rendszerek nem téveszthetők össze a Magyar Honvédség által újonnan hadrendbe állított, folyamatos fejlesztéseken

végbemenő C2 rendszerével. A C2 rendszer egy komplex parancsnoki vezetés-irányítási rendszer, amely olyan információk gyűjtését, feldolgozását és tárolását hivatott kiszolgálni, mely a parancsnok döntéshozatalát könnyíti és gyorsítja meg a hadműveleti feladatok végrehajtása során.

A válságreagáló műveletek híradó- és informatikai rendszere tehát azon eljárások, technikai eszközök és az azokat telepítő, üzemeltető személyzet komplex rendszertechnikai összessége, amely a válságreagáló műveletekben résztvevő erők belső-, a szervezetek közötti-, a nemzeti (honi)- és a hadműveleti elöljárók irányában biztosítja az információcserét és annak feldolgozását a többnemzeti jellegből adódó követelmények megteremtése érdekében.

Fontos alapelv, hogy a híradó- és informatikai rendszer kialakítása során figyelembe kell venni a vezetés egységét és folyamatosságát, a decentralizációt valamint az együttműködést. A továbbiakban a híradó- és informatikai rendszert az előzőekben leírtaknak megfelelően értelmezve alkalmazzuk, amely véleményünk szerint jól tükrözi mindazon informatikai és kommunikációs (híradó) rendszereket, amelyek a vezetés és irányítás támogatását képezik a missziós feladatok végrehajtása során.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Napjainkban a legnagyobb veszélyt a kisméretű fegyveres összecsapások jelentik, amelyek nem csupán a régió, de a világ biztonságát is nagymértékben befolyásolják. Ezen válságok rendezése korszerű szemléletet, és korszerű fegyverzettel, haditechnikai eszközökkel felszerelt erőket követel meg a NATO minden tagállamának haderejétől. A NATO megfogalmazása alapján a válságok kezelése érdekében összetett, többfunkciós válságreagáló műveletek kerülnek végrehajtásra, amelyek a kialakult konfliktus kezelésére, esetlegesen megelőzésére, azaz válságkezelésre irányulnak, katonai, civil és egyéb rendészeti erők és eszközök felsorakoztatásával.

A siker kivívásának alapvető eleme, hogy a determinált célokhoz hozzá kell rendelni a válságreagáló erők képességeit. A washingtoni szerződés és a NATO-csúcsértekezletek meghatározták azokat a főbb irányelveket, amelyek biztosítják a sikeres missziós tevékenységeket. A legalapvetőbb képességek mellett – mint a mobilitás, rugalmasság, telepíthetőség – a fő hangsúly a korszerű infokommunikációs eszközökkel támogatott vezetésen van. A NATO és a nemzeti fejlesztéseknek ezen elvárásoknak kell megfelelnie, amelyek természetesen a műveleti tapasztalatok alapján folyamatosan bővülnek, pontosításra kerülnek. Ezért a folyamatosan megjelenő új kihívásokra történő gyors és hatékony reagálás érdekében képesnek kell lenni felismerni és meghatározni az irányelveket, eszközöket, amelyek alkalmazásával elérhetőek a kitűzött célok. Mindezek mellett a magas fokú együttműködő képesség – technikai és személyi – elengedhetetlen eleme a többnemzeti műveletek sikerének.

A vállalt kötelezettségeknek megfelelően a Magyar Honvédség részt vesz különböző nemzetközi műveletekben. Hozzájárul a szövetséges küldetések ellátásához az arra kijelölt és felkészített katonai erők felajánlásával, elősegítve a terrorizmus elleni harc katonai feladatainak ellátását. Ezek elérése érdekében folyamatos fejlesztések kerülnek végrehajtásra, amelyek a válságreagáló műveletekben szolgálatot teljesítő alegységek védelmét, és a sokrétű feladatok ellátását biztosítja. Az alegység folyamatos vezetése érdekében olyan híradó- és informatikai rendszert kell létrehozni, amely támogatja a parancsnoki vezetést a műveletek teljes spektrumában, biztosítja az információcserét, azok feldolgozását és esetleges tárolását a művelet végrehajtásának időtartamában. A többnemzeti műveletek során megtervezésre, megszervezésre, telepítésre és üzemeltetésre kerülő híradó- és informatikai rendszer számos követelményeknek kell, hogy megfeleljen, amelyeket elsősorban a missziós tevékenységet ellátó erők képességei határoznak meg.

A közleménnyel kapcsolatos következtetéseink alapján megállapítható, hogy a nemzetközi műveletek sikeres végrehajtása érdekében szövetségesi és nemzeti szinten egyaránt meg kell határozni mindazon képességeket, amelyek szavatolják az összetett feladatrendszer eredményes ellátást a hadműveleti területen.

A nemzetközi- és hazai missziós tapasztalatok alapján megállapítható, hogy kisméretű, többfunkciós képességekkel rendelkező, korszerű haditechnikai eszközökkel felszerelt, civil képességek kiegészített katonai erőket kell létrehozni, melyek a kor követelményeinek megfelelően – az elvárásokhoz igazítva – viszonylag kis anyagi ráfordítással továbbfejleszthetők, és a jellegükből adódóan képesek a konfliktusok felszámolására és hazai alkalmazásra egyaránt.

A legfontosabb képességek közé tartozik a gyors bevethetőség, a moduláris felépítés, expedíciós képesség, rugalmasság és a mindezt támogató, korszerű híradó- és informatikai rendszerrel való kiegészítés.

A modern híradó és informatikai eszközökkel megszervezett híradó- és informatikai rendszer támogatja a parancsnok és törzse részére a vezetést, amely a széleskörű információcserét és információfeldolgozást lehetővé téve elősegíti a siker kivívását. Ezen rendszerek kiemelt jellemzője kell, hogy legyen a nemzetközi együttműködő képesség, amely a többnemzeti jellegből adódóan releváns.

A válságreagáló műveletek híradó- és informatikai rendszere azon eljárások, technikai eszközök és az azokat telepítő, üzemeltető személyzet komplex rendszertechnikai összessége, amely a válságreagáló műveletekben résztvevő erők belső-, a szervezetek közötti-, a nemzeti (honi)- és a hadműveleti elöljárók irányában biztosítja az információcserét és annak feldolgozását, a többnemzeti jellegből adódó követelmények megteremtése érdekében.

FELHASZNÁLT IRODALOM

[1] Resperger István: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során (doktori PhD értekezés) Budapest, 2001 p.: 34.

[2] Kőszegvári Tibor: A válságkezelés aktuális problémái, ZMKA Közlemények, 1994, 202. szám; p.217.

[3] Deák János: Napjaink és a jövő háborúja, Hadtudomány a Magyar Hadtudományi Társaság folyóirata XV. évfolyam 1. szám (2005. március) (ISSN: 1215-4121)

[4] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás, Honvédelmi Minisztérium kiadványa, 2010; p.: 27-28.

[5] Rábai Zsolt: Viták az új stratégiai koncepció körül, A NATO formálódó új stratégiai koncepciója és Magyarország; Konferencia előadás 2010. március 25.; ZMNE Budapest

[6] Bencze Balázs–Hegedüs Zoltán–Kolossa Sándor–Padányi József–Praveczki Zoltán–Szternák György: A Válságreagáló műveletek elmélete és gyakorlata a 21. században, Egyetemi jegyzet; ZMNE Budapest 2004; p.: 66.

[7] Sticz László – Csák Zoltán: Az expedíciós képesség és műveletek tartalmi elemeinek vizsgálata, http://www.hm.gov.hu/files/9/9988/03.pdf (letöltve: 2008.10.18.)

[8] 51/2007. (VI. 6.) OGY határozat a Magyar Honvédség további fejlesztésének irányairól, Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 69. szám; 2007. június 6.; p.: 4901

[9] Szenes Zoltán: Politikai viták – lehetséges katonai következmények, A NATO formálódó új stratégiai koncepciója és Magyarország; Konferencia előadás 2010. március 25.; ZMNE Budapest

[10] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal)

[11] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás, Honvédelmi Minisztérium kiadványa, 2010; p.: 52.

[12] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal)

Horváth Zoltán
horvath.zoltan@zmne.hu

URH ÉS MIKROHULLÁMÚ FÖLDFELSZÍNI PONT-PONT RÁDIÓ-ÖSSZEKÖTTETÉS TERVEZÉSÉNEK TÁMOGATÁSA HULLÁMTERJEDÉSI MODELLEK ALKALMAZÁSÁVAL

Absztrakt

Az URH és mikrohullámú földfelszíni pont-pont rádió-összeköttetés tervezése nem egyszerű feladat. A domborzat figyelembe vétele, időigényes, szubjektív hibákkal terhelt. Nem elegendő az optikai láthatóság vizsgálata. A szerző bemutatja azokat az algoritmusokat, melyek a rádió-összeköttetés automatizált tervezését elősegíti.

Not so easy task to plan a radio connection between two points, close to the surface used VHF or higher frequencies. To count the the effect of the terrain over the radio connection is too consumptive of time and involved of subjective mistakes. The monitoring of optical visibility is not enough in this case. The author show us that algorithms which ones conduce to plan radio connection by automated proceedings.

Kulcsszavak: *URH, mikrohullám, rádió-összeköttetés, automatizált tervezés ~ VHF, radio connection, automated planning*

1. A RÁDIÓCSATORNA, MINT EGY RENDSZER KRITIKUS ELEME

A rádiórendszerek egyes elemeinek, rendszertechnikai részegységeinek vizsgálata során belátható, hogy összeköttetés tervezése szempontjából az átvitel „leggyengébb láncszeme” a *rádiócsatorna*.

Míg a többi rendszerelem emberi tervezés eredménye, tulajdonságaik jól meghatározhatóak, addig a rádiócsatorna tulajdonságainak vizsgálatára, befolyásolására kevés lehetőség áll rendelkezésre.

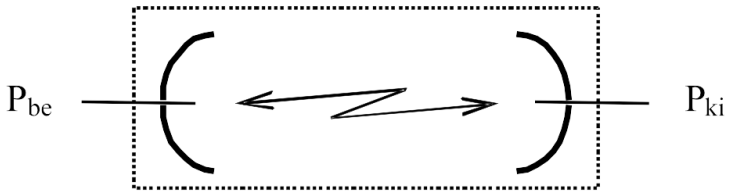
A rádiócsatorna az adóantenna bemenete és a vevőantenna kimenete közötti kétkapu (1. ábra), melynek csillapítása a szakaszcsillapítás.

Az antennák egyik fő feladata a rádiórendszerekben a jelátalakítás. Az adóantenna a bemenetére juttatott, vezetett hullámot alakítja át térhullámmá, a vevőantenna a térhullámot alakítja vissza vezetett hullámmá. Az adó- és vevőantenna közötti térrészben a rádióhullámok közvetítő közeg nélkül, a rádiócsatornában haladnak.

Az adó- és a vevőantenna közötti térrészben a rádióhullámok többféle mechanizmus útján terjedhetnek. URH és mikrohullámú frekvenciatartományban a talaj csillapító hatása olyan nagy, hogy a felületi hullámú terjedési mód figyelmen kívül hagyható, az összeköttetés gyakorlatilag térhullámokkal jön létre.

A föld felszínéhez közeli két pont között számos terjedést módosító tényezővel kell számolni, mint a föld véges vezetőképessége, görbültsége, domborzat hatása, a föld felületéről történő visszaverődés hatása, a légkör törésmutatójának magasságfüggése. Meg kell vizsgálni (reflexió, diffrakció), hogy meddig használható a számítások során a geometriai optika.

A földfelszín fölötti optikai rálátás önmagában nem elegendő a szabadtéri térerősség jelenlétéhez.



1. ábra: A rádiócsatorna

A rádiócsatorna szakaszcsillapítása (a_{sz}):

$$a_{sz} = 10 \cdot \lg\left(\frac{P_{be}}{P_{ki}}\right) \quad [dB]$$

ahol: P_{be} bemeneti teljesítmény
P_{ki} maximális kivehető hatásos teljesítmény

2. SZAKASZCSILLAPÍTÁS BECSLÉSE EGY HULLÁMTERJEDÉST GÁTLÓ AKADÁLY ESETÉN

Amennyiben egy akadály terheli a rádiócsatornát, a szakaszcsillapítás számítása során figyelembe kell venni a diffrakciós fadinget.

A diffrakciós fading:

$$L[dB] = 20 \cdot \lg\left|\frac{E}{E_0}\right|$$

ahol: E a fading által csökkentett térerősség
E_0 a szabadtéri térerősség

Ez alapján a szakaszcsillapítás:

$$a_{sz} = a_0 - L\ [dB]$$

ahol: a_0 a szabadtéri csillapítás
L az akadály(ok) okozta diffrakciós fading

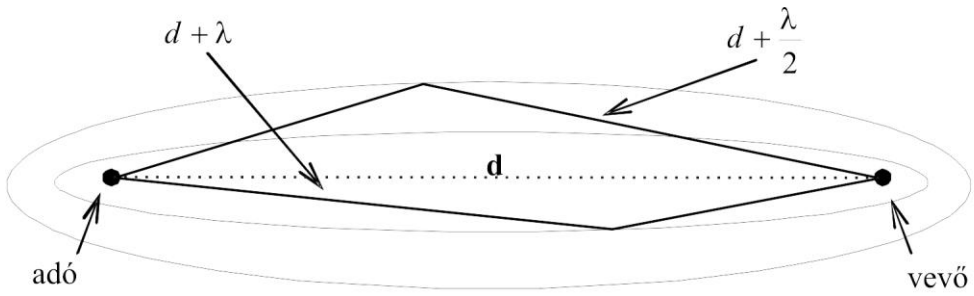
A Huyghens-elv alapján a hullámterjedés a hullámfrontban található elemi centrumok útján jön létre. Ha a forrás és a vizsgált pont köré ellipszoidsereget rajzolunk (2. ábra), melynek nagytengelyei (b) rendre:

$$b = d + k \cdot \frac{\lambda}{2}$$

ahol: d a forrás és a vizsgált pont távolsága
k természetes szám
λ hullámhossz

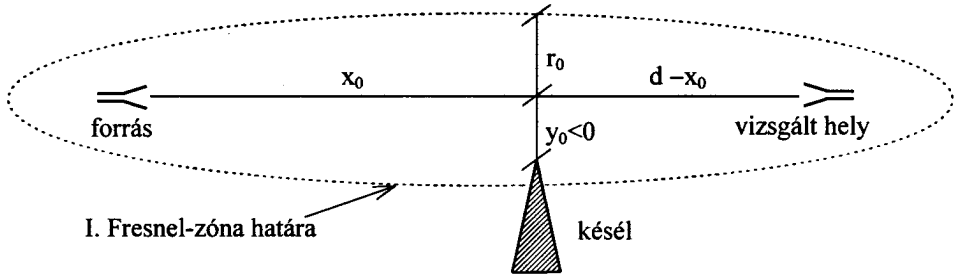
A Fresnel-ellipszoidok által zónázott azonos zónában található elemi centrumok egymás hatását erősítik, az egymással szomszédos zónában található elemi centrumok egymás

hatását gyengítik. A legbelső zónától (I. Fresnel-ellipszoid) eltekintve az egyes zónák egymás hatását gyakorlatilag semlegesítik.



2. ábra: Fresnel-zónák

A 3. ábrán látható a rádiócsatorna vertikális síkmetszete. Igen jó közelítéssel (horizontális terjedést feltételezve) x_0 helyen az I. Fresnel-zóna sugara (r_0):



3. ábra: A késéldiffrakció paraméterei

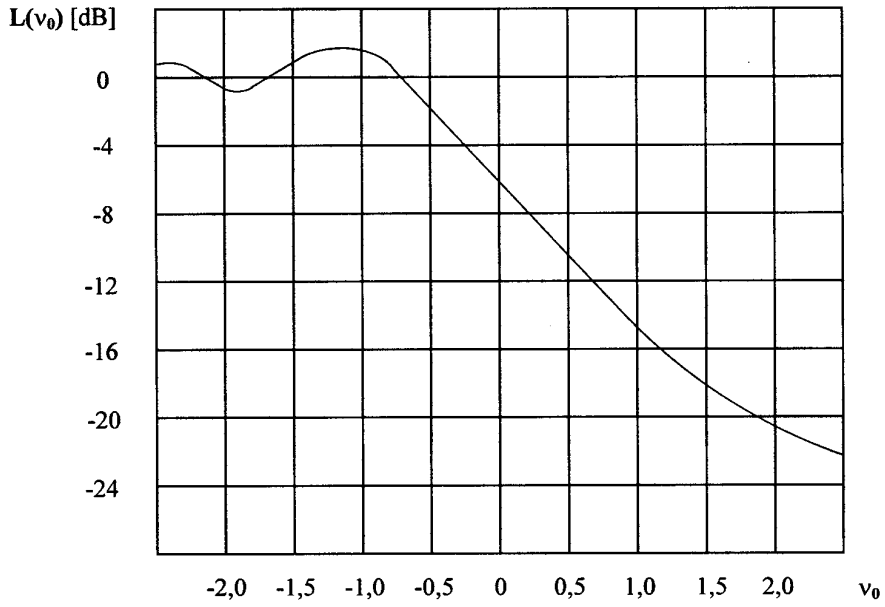
$$r_0 = \sqrt{\lambda \cdot \frac{x_0 \cdot (d - x_0)}{d}}$$

ahol: λ az üzemi hullámhossz
d az összeköttetés távolsága

A 3. ábra alapján az I. Fresnel-zónába a benyúlás mértéke (ν_0):

$$\nu_0 = \frac{y_0}{r_0}$$

A késél okozta fading a benyúlás mértékének függvényében a 4. ábrán látható. Kiszámítva (ν_0) értékét az egy késél okozta fading ($L(\nu_0)$) meghatározható:



4. ábra: Késél okozta fading

$L(\nu_0)$ függvény értelmezési tartományát felosztva az egyes tartományokhoz közelítő-függvény rendelhető, mely segítségével (ν_0) ismeretében L számítható.

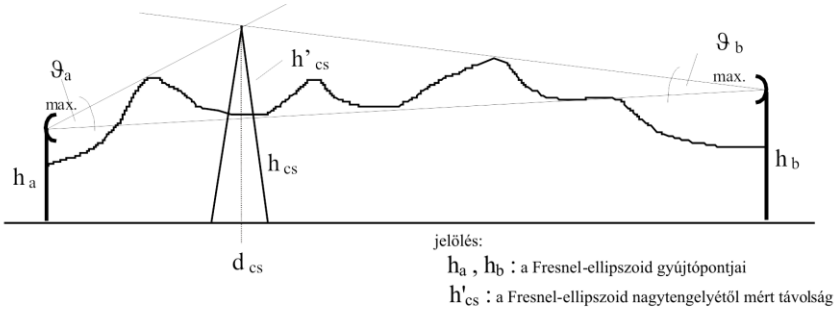
Ezek a függvények a következők:

$$L_{(\nu_0)[dB]} = \begin{cases} 20 \cdot \lg(1) & \nu_0 \in (-\infty;-0{,}8) \\ 20 \cdot \lg(0{,}5 - 0{,}62 \cdot \nu_0) & \nu_0 \in [-0{,}8;0) \\ 20 \cdot \lg(0{,}5 \cdot 10^{-0{,}95\nu_0}) & \nu_0 \in [0;1) \\ 20 \cdot \lg\left(0{,}4 - \sqrt{0{,}1184 - (0{,}38 - 0{,}1 \cdot \nu_0)^2}\right) & \nu_0 \in [1;2{,}4) \\ 20 \cdot \lg\left(\dfrac{0{,}225}{\nu_0}\right) & \nu_0 \in [2{,}4;\infty) \end{cases}$$

3. SZAKASZCSILLAPÍTÁS BECSLÉSE TÖBB HULLÁMTERJEDÉST GÁTLÓ AKADÁLY ESETÉN

Rendszerint a rádiócsatornát nem egy, hanem több akadály terhel. A többszörös késél okozta diffrakció számítás valamennyi algoritmusának alapjául az egyetlen késélre vonatkozó fading számítása szolgál. A különbség az egyes késélek figyelembevételében, a késélek egymásra hatásának modellezésében van. Négy terjedési modellt vizsgáltam.

A *Bullington modell* a rádiócsatorna két végpontjából a legmagasabb helyszög adat látható két késél felhasználásával, egyeneseket fektetve az adó és közeli késéle, valamint a vevő és közeli késéle csúcsára, az egyenesek metszéspontja jelöli ki egy virtuális késél helyét és csúcsát (5. ábra). Ez a megoldás igen durva megközelítést jelent.

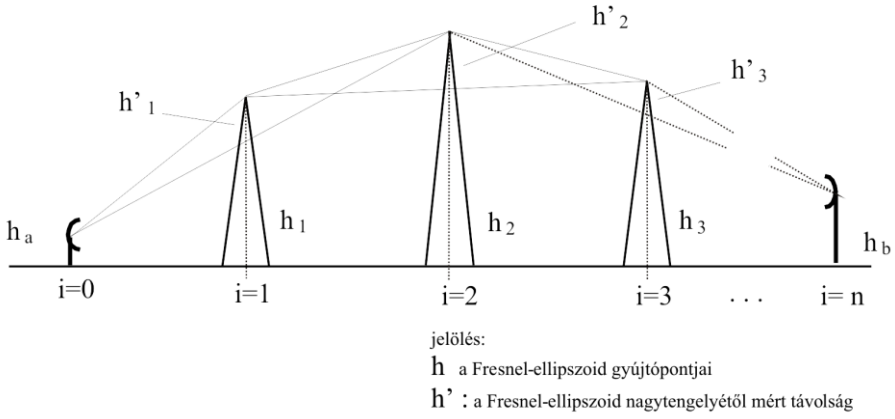


5. ábra: Bullington modell

A szakaszcsillapítás:

$$a_{sz} = a_0 - L\left(h_a; h_{cs}\{\vartheta_{a\max}; \vartheta_{b\max}\}; h_b\right)$$

Ennél lényegesen jobban használható az *Epstein-Peterson modell*. A rádiócsatorna egyik végpontjából a másik irányba haladva az egyes késélek okozta fadinget a szomszéd késélek csúcsaira, mint virtuális adó, illetve vevőpontra számítja, majd az eredő diffrakciós fading ezek összege (6. ábra). Ez a modell túlbecsüli a térerősséget, tehát alábecsüli a csillapítást, ezért EMC vizsgálatoknál használatos.



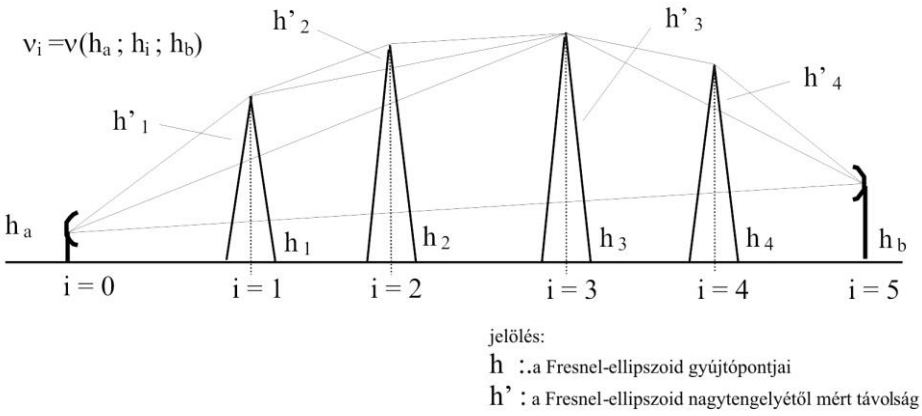
6. ábra: Epstein-Peterson modell

A szakaszcsillapítás:

$$a_{sz} = a_0 - \sum_{i=1}^{n-1} L\left(h_{i-1}; h_i; h_{i+1}\right)$$

Ennek ellenpéldája a szintén gyakorlatban is használatos *Deygout modell*. A rádiócsatornában a benyúlás mértéke alapján kiválasztja a legdominánsabb késélt. Ezt

követően, kiszámítva a hozzátartozó fadinget a domináns késélnél kétfelé választja a rádiócsatornát. Az algoritmus az adó, illetve a vevőantenna felé mindaddig folytatódik, míg a virtuális rádiócsatornák késélt tartalmaznak (7. ábra).



7. ábra: Deygout modell

A szakaszcsillapítás:

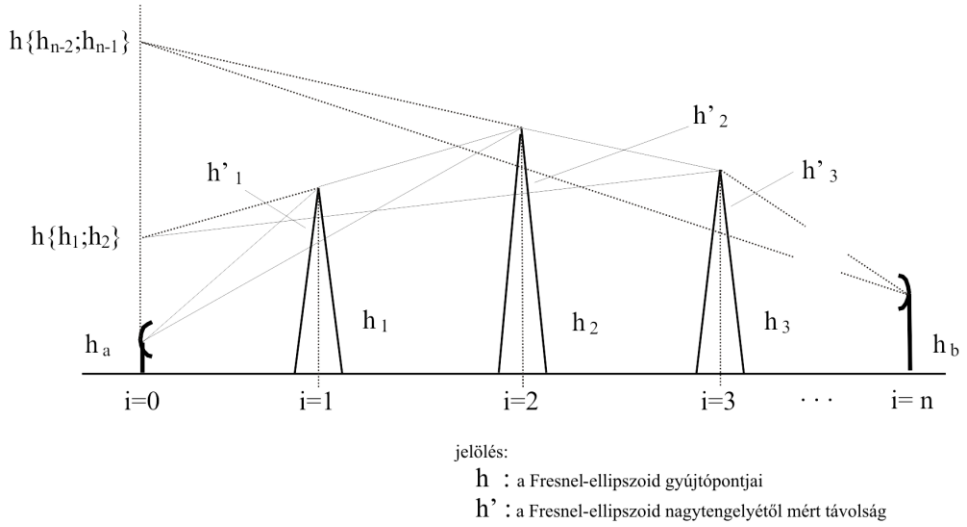
$$a_{sz} = a_0 - \sum_{i=1}^{n-1} L(\nu_i)$$

ahol (a 7. ábra alapján, feltételezve, hogy $\nu_3 > \nu_1 > \nu_2$ *és* $\nu_3 > \nu_4$):

$\nu'_3 = \nu(h_a ; h'_3 ; h_b)$;
$\nu'_1 = \nu(h_a ; h'_1 ; h_3)$;
$\nu'_2 = \nu(h_1 ; h'_2 ; h_3)$;
$\nu'_4 = \nu(h_3 ; h'_4 ; h_b)$;

Programozás-technikailag az eljárás rekurzív algoritmust eredményez. A módszer túlbecsüli a szakaszcsillapítást, tehát alábecsüli a térerősséget, ezért összeköttetések számításánál használatos.

Epstein-Peterson és Deygouth módszerén kívül a gyakorlatban még a *Japán modell* használatos. Epstein-Peterson módszeréhez hasonlóan a rádiócsatorna egyik végpontjától (adó) indul a másik végpont (vevő) felé. Az egyes késélek okozta fading értékét úgy határozza meg, hogy a virtuális vevőt a vizsgált késélt sorrendben követő késélre helyezi. Az adó pozícióját nem változtatja, viszont az adó virtuális magasságát a vizsgált és az azt sorrendben megelőző késélek csúcsaira fektetett egyenes adó antenna helyén kimetszett magassága adja (8. ábra).



8. ábra: Japán modell

A szakaszcsillapítás:

$$a_{sz} = a_0 - \sum_{i=1}^{n-1} L\left(h\{h_{i-1};h_i\};h_i;h_{i+1}\right)$$

Ez a modell Epstein-Peterson és Deygouth módszerével számított csillapítás értékeinek köztes értékét adja, de az eredmény a vizsgálat irányára nem szimmetrikus

ÖSSZEFOGLALÁS

Megvizsgálva a különböző hullámterjedési modelleket megállapítható, hogy URH és mikrohullámú földfelszíni pont-pont összeköttetés esetén – térhullámú terjedést feltételezve – nem elegendő az optikai láthatóság vizsgálata. Az egy késél okozta többletcsillapítás számítása kidolgozott, erre épülve számos terjedési modell létezik. A modellek jól algoritmizálhatóak.

Az említett modellek alkalmazása napjainkban egyre szélesebb körben megvalósul. A térképi információk digitális formában történő elérhetősége, feldolgozhatósága lehetőséget biztosít ezen modellek tervező munkába történő alkalmazására. A térinformatikai alapú tervező, elemző munka ezáltal gyorsabbá, olcsóbbá, megbízhatóbbá válik és új minőséget rejt magában.

FELHASZNÁLT IRODALOM

- J. D. Parsons: The Mobile Radio Propagation Channel, Pentech Press, London, 1992;
- Wireless Communication, Radio Propagation modells, (http://people.deas.harvard.edu/~jones/es151/prop_models/propagation.html);
- Dr Istvánffy Edvin: Tápvonalak, antennák és hullámterjedés, Tankönyvkiadó, Budapest, 1967;
- Géher Károly fsz.: Híradástechnika, Műszaki könyvkiadó, Budapest, ISBN 963 160173 0.

Sándor Miklós – Kuris Zoltán
sandor.miklos@zmne.hu – zoltan.kuris@bm.gov.hu

A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELEM ÉS A VÉDELMI CÉLÚ KATASZTRÓFAVÉDELMI HÍRADÁS KAPCSOLATRENDSZERE

Absztrakt

Az információs társadalom működésének zavarai, katasztrófavédelmi és különböző minősített helyzet kialakulásához vezethetnek. A szerzők a társadalmi szintű megközelítést követően, részleteiben fejtik ki a Kritikus Információs Infrastruktúra működési zavarainak hatásait a létfontosságú infrastruktúrákra. Bizonyítani szeretnék, hogy a kialakuló katasztrófavédelmi és egyéb minősített helyzetekben, különösen fontos és nélkülözhetetlen az infokommunikációs rendszerek megbízható működésére alapozott katasztrófavédelmi híradás zavarmentes üzemelése. Az információs stabilitás fogalmának bevezetésén keresztül mutatják be a rendszerközpontú működtetés alapvető irányelveit.

A catastrophy might emerge from the disorders of the informational society. The social effects are analysed. Then the disorders of the critical infrastructure of information is described in detail, How they affect the infrastructures of vital importance the authors describe it in detail. The significance and functioning of sending news are proved as well as the significance of notifying news.

Kulcsszavak: *Kritikus Információs Infrastruktúra Védelem, minősített adat, fizikai biztonság, elektronikai biztonság, dokumentum biztonság, személyi biztonság, Az európai unió létfontosságú infrastruktúrák figyelmeztető és információs hálózata ~ Marathon Terra; K-600/KTIR, Trans European Services for Telematics between Administrations,CIWIN, TESTA, sTESTA*

BEVEZETÉS

Ma már alapvető axiómának tekinthető az, hogy a biztonság újkori értelmezésének megfelelően, a biztonság dimenzióinak rendszere – az elemek közötti kapcsolatrendszer – alapvetően átalakult. Bizonyos biztonsági dimenziók felértékelődtek, más dimenziók pedig veszítettek súlyukból. Különösen igaz ez, amikor az utóbbi évtized változásait, az információs társadalom működésének tükrében vizsgáljuk. Ma a modern társadalmak nagy része felismerte annak jelentőségét, hogy a társadalom zavartalan működését biztosító „létfontosságú infrastruktúrák" működtetése alapvető biztonságpolitikai cél. Ennek megfelelően a modern társadalmak, a biztonsági stratégiájuk megfogalmazásakor különös figyelmet tanúsítanak az újkori kihívások, kockázatok és fenyegetések részletes feltárására. Az információs társadalmi formációban működő államoknak különös figyelemmel kell lenniük tehát a létfontosságú infrastruktúráik és információs infrastruktúráik védelmére, mert a védelmi rendszer egyenszilárdságának csökkenése alapvetően képes befolyásolni az adott ország geopolitikai és geostratégiai helyzetét egyaránt. A biztonsági stratégia a társadalom működésének biztosítására irányuló alapvető dokumentum. A hazai biztonsági stratégiát elemezve megállapítható, hogy hazánk a fent említett új kori követelményrendszerre építkező, megfelelő biztonsági stratégiával rendelkezik. Ha tovább vizsgáljuk az ágazati stratégiák rendszerét, megállapítható hogy igen ritka a pragmatikus, rendszerszemlélettel rendelkező ágazati stratégia.

Az általános biztonságpolitikai szemléletű megközelítést követően célszerű megvizsgálni azt, hogy a létfontosságú infrastruktúrák zavartalan működtetését célzó Kritikus Infrastruktúra védelem (a továbbiakban: KIV) milyen kapcsolatban van a Katasztrófavédelmi területtel, illetve milyen szerepe van ezen a területen a Kritikus Információs Infrastruktúrák (a továbbiakban KIIV) zavarmentes üzemeltetésének. Érdemes azt is vizsgálni, hogy ezen a területen hogyan valósul meg, - vagy milyen igény mutatkozik - a vezetési irányítási, távközlési és informatikai, rendszerek komplex rendszerének alkalmazásának. Elfogadható állítás az, hogy a társadalom információs és infokommunikációs rendszereinek rendelkezésre állása ugrásszerűen felértékelődik, katasztrófavédelmi és a minősített időszak helyzetében. Célszerű tehát azt vizsgálni, hogy milyen jogalkotási, szabályozási és technológiai feladatok körvonalazódnak ezen a területen. A fentiekből következik, hogy azt is célszerű megvizsgálni, hogy a fentiekben kifejtett vezetés-irányítási, távközlési és informatikai rendszerek, milyen előfeltételekkel és környezetben tudják biztosítani azt az információs stabilitást, bonyolult katasztrófavédelmi és minősített helyzetben.

1. A BIZTONSÁG ÚJKORI DIMENZIÓI

A biztonság fogalmának néhány definícióját az alábbiakban szükséges összefoglalni annak érdekében, hogy az újkori dimenziókat értelmezni tudjuk.

A szó eredetét illetően, a latin securus, securitas: sine-nélkül + cura-aggodalom, félelem összetételéből ered. Tovább fűzve a gondolatat, egy változatban az alábbiak szerint lehet értelmezni a biztonságot:

- *Egyrészt. fenyegetettség hiánya (abszolút);*
- *Másrészt, olyan állapot, ahol kizárhatók, vagy megbízhatóan kezelhetőek a fenyegetések.*

Ezzel összefüggésben a biztonságérzet: veszély, kockázat érzékelése (szubjektív).

A Külföldi szakirodalomban a biztonság fogalmának általános megfogalmazása így hangzik:

„A biztonság fizikai a fizikai veszély hiányát, vagy az e veszéllyel szembeni védelmet jelenti." [1]

Az Amerikai Egyesült Államok szakirodalmából idézve, pedig így hangzik:

„A nemzetbiztonság nemcsak lakosságunk és területünk védelme a közvetlen támadástól, hanem létfontosságú gazdasági és politikai érdekeink védelme is különféle eszközökkel." [2]

A *Hadtudomány 2007/1 számában* megfogalmazottak szerint a biztonságelmélet új fogalmára közölt meghatározást. Ennek analógiájára: a biztonságelmélet a legtágabb értelemben a nemzeti, a nemzetközi biztonságot befolyásoló kihívások, veszélyek és kockázatok megszüntetésére, a lehető legkisebb szintre mérséklésére hivatott nemzeti, szövetségi, regionális, nemzetközi szervezetek tevékenységének sikerét meghatározó, elméleti tételeket és gyakorlati tapasztalatokat összefoglaló ismeretrendszere. [4]

A *Hadtudomány 2006/3 számában* [5] biztonság kérdéseivel foglalkozó cikk szerzője egy kutatónak ebben a kérdésben kifejtett véleményét összegezve írja, *hogy „azon túlmenően, miszerint a statikus állapotnak tartott biztonságot komplex rendszerként értelmezi, a biztonság meglétét az esetleges veszélyek leküzdésére való képességgel, az erre való felkészültséggel köti össze. Ezzel a biztonság nem egyszerűen állapot, hanem egy olyan cél, amelynek eléréséhez aktivitásra, cselekvésre van szükség."*

Az 1985-ben kiadott német Biztonságpolitikai Szótár az alábbiakat tartalmazza:

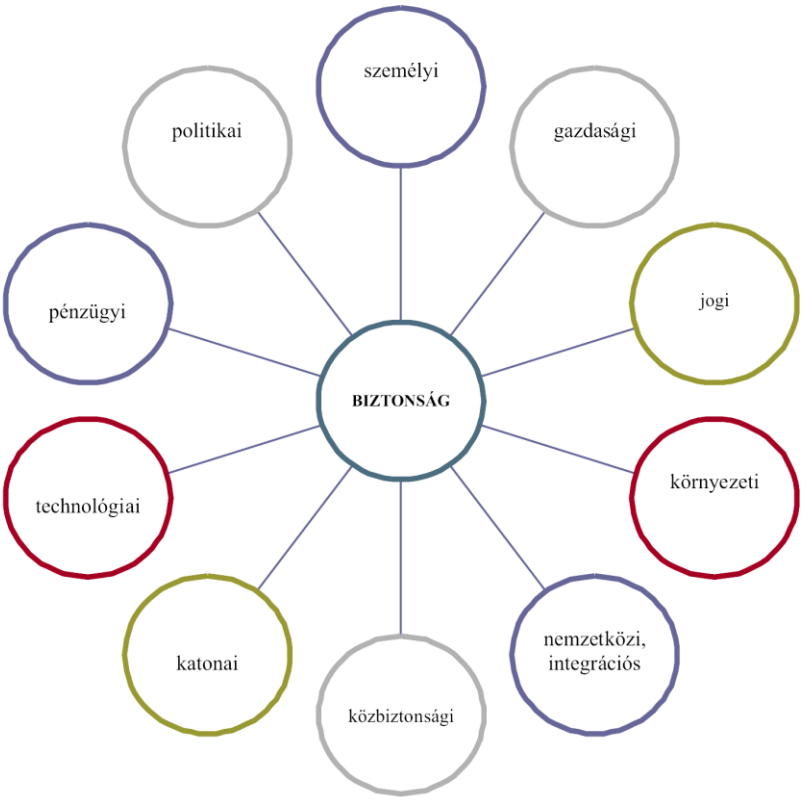
- *A biztonság nem más, mint a veszély hiánya;*
- *a biztonság az egyes emberek vagy azok csoportjainak, az államoknak és az államcsoportoknak a bizonyossága arról, hogy a lehetséges veszélyektől védve vannak;*
- *a biztonság olyan állapot, amelyben az egyéneket, csoportokat és az államokat komoly veszélyek nem fenyegetik, illetve azoktól védettnek érzik magukat, vagy – pozitívan kifejezve – amelyben biztosak abban, hogy jövőjüket saját elképzelésük szerint alakítják. A biztonság és a fenyegetettség foka jelentős mértékben függ tehát a szubjektív érzettől, a történelmi tapasztalattól, az önmegértéstől és a környezethez való viszonytól.* [6]

Végül a Magyar Hadtudományi Lexikon szerint *„a biztonság az egyének, csoportoknak, országoknak, régiónak (szövetségi rendszereknek) a maguk reális képességein és más hatalmak nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete (és annak tudati tükröződése), amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkezhető veszély, illetve adottak az ellene való eredményes védekezés feltételei."* [6]

A fentiekből látható, hogy a biztonságot az államok manapság komplex módon értelmezik. Az elemek fontossági sorrendben: a politikai, gazdasági szociális ökológiai és katonai területek. Természetesen ez béke állapotra jellemző fontossági sorrend és az adott körülményeknek megfelelően a súlypontok áthelyeződhetnek. A fenti elemeket megvizsgálva következtetés eredménye ként egyértelműen megállapítható, hogy a fenti elemek megjelenésének színterei a különböző létfontosságú infrastruktúrák és ezen belül a kiemelt fontosságú szektorok.

Ahhoz, hogy a biztonság hatókörét értelmezni tudjuk meg kell határozni a tartalmát. Ezzel összefüggésben a biztonság szintjei, *az egyének, csoportok, kisebbségek, nemzetek, államok, régiók és a nemzetközi rendszer.*

Ugyanakkor a 90'-es évektől elterjedt a biztonság fogalmának parttalan használata, kiterjedt azon jelenségek köre, amelyek kiváltói lehetnek a már elemzett biztonsági hiányérzetnek. Ezért szükséges és elégséges értelmezés szerint az alábbi biztonsági dimenziók körvonalazódnak.



1. ábra: Jellemző biztonsági változatok

A társadalom biztonsági érzete összességében mérhető jelenség. E mérés és a biztonsági érzetek meghatározására hívták segítségül a biztonságpolitikával foglalkozó szakemberek a szociológia eszköztárát. A TIT HABE[1] (a honvédelmi tárca megbízásából) a Szonda Ipsos-sal közösen két ízben is végzett közvélemény-kutatást e terület vonatkozásában. 1999-ben ezer, míg 2008-ban háromezer főt kérdeztek meg „az utca emberei közül”! A következő táblázat ennek rövid összefoglalását szemlélteti.

1 A TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesületet életünk legfontosabb kérdéseivel, a biztonsággal és biztonságpolitikával foglalkozik az ország egész területén. A TIT HABE 1996-os megalakulása óta aktívan részt vesz az ország kül-és biztonságpolitikájával, NATO- és EU-tagságával és a nemzetközi biztonság erősítése érdekében végzett egyéb tevékenységével összefüggő kérdések elemzésében és publikálásában, hazai és nemzetközi rendezvények szervezésében, a lakosság különböző célcsoportjainak a tájékoztatásában és felkészítésében.

2. ábra, Forrás: Gondolatok és vélemények a biztonságunkról – a biztonságkultúra kérdései, TIT HABE, 2008[2]

A biztonság a fejlődés előfeltétele.

A konfliktusok nemcsak az infrastruktúrákat – így a szociális infrastruktúrákat – teszik tönkre, hanem ösztönzik a bűnözést, eltántorítják a befektetőket és lehetetlenné teszik valamennyi szokásos gazdasági tevékenység gyakorlását is. Számos ország és régió a konfliktus–bizonytalanság–szegénység ördögi körének a foglya.

A fenti rövid áttekintés jól példázza, hogy a társadalom működését biztosító infrastruktúrák működésében előforduló zavarok visszahatnak a társadalom biztonsági érzetére és alapvető hatással vannak a társalmi fejlődésre is!

2. AZ INFOKOMMUNIKÁCIÓS RENDSZEREK INFORMÁCIÓBIZTONSÁGI STABILITÁSÁT BIZTOSÍTÓ ÖSSZETEVŐK ELEMZÉSE

Az információs társadalom nagyon fejlett és hatékony társadalom, ugyanakkor meglehetősen sebezhető is. Sebezhetőségének alapját az adja, hogy működése szorosan kapcsolódik a globális, nemzeti, regionális és lokális információs környezethez [h 67.old.] Irányadó szakemberek szerint, napjainkban várhatóan felértékelődik az információs környezet átfogó védelme. A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2073/2004. (IV.15.) Korm. határozat [3] a fenyegetések, kockázatok, kihívások szakaszában (II.) nevesíti az információs társadalom kihívásait, ezen belül a telekommunikációs hálózatok sebezhetőségét és kockázatait emeli ki. A terrorizmus elleni védekezés szakaszban (III.3.1) külön kiemeli a

2 Dr. Radványi Lajos szociológus, biztonságpolitikai szakértő, a TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesület alelnöke „A magyar lakosság biztonságfelfogásának változásai 1999 – 2008” című előadásából. Veszélyhelyzetek kezelésének kormányzati koordinációja – munkaműhely, Göd, 2009. március 10.

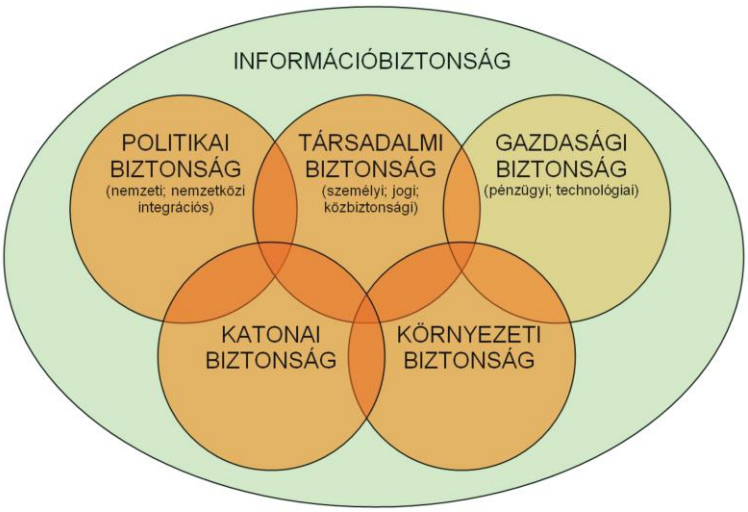
kritikus infrastruktúrák védelmének feladatait is. Az információs rendszerek védelme szakaszban (III.3.7) pedig hangsúlyozza a kormányzati információs rendszerek védelmének szükségességét és felhívja a figyelmet a sikeres védelem érdekében szükséges együttműködésre, az érintett informatikai és távközlési szolgáltatókkal. Sajnos a Magyar Köztársság Nemzeti Biztonsági Stratégiájával összefüggő ágazati (távközlés, informatika) területét fellelő gyűjtő néven infokommunikációs doktrínának [8] nevezhető dokumentum a mai napig nem került kidolgozásra.

A Magyar Köztársaság kritikus információs infrastruktúrái az alábbiak:

- Informatikai rendszerek és hálózatok;
- automatizálási, vezérlési és ellenőrzési (SCADA, távmérő, távérzékelő és telemetriai) rendszerek;
- internet szolgáltatás és infrastruktúrája;
- vezetékes távközlési szolgáltatások és infrastruktúrái;
- mobil távközlési szolgáltatások és infrastruktúrái;
- műholdas távközlési szolgáltatás és infrastruktúrái;
- földfelszíni műsorszórás és infrastruktúrája;
- közigazgatási informatika és kommunikáció és infrastruktúrái;
- a kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei.

A biztonság dimenzióiban értelmezett információbiztonsággal összefüggésben megállapítható, hogy a KIV szektoraiban gyűjtött, feldolgozott tárolt és továbbított információkat a különféle infokommunikációs eszközök alkalmazásával kezeljük. Infokommunikációs eszközök gyűjtőfogalom kőré csoportosíthatóak, az informatikai és a távközlés, illetve az egyéb információtechnológiai eszközök konvergenciájának következményeként alkalmazott „informatizálódott” eszközök. A fenti infokommunikációs rendszerek információbiztonsági stabilitásának biztosítása alapfeltétel, a katasztrófavédelmi és egyéb minősített időszaki helyzetekben is. Az előző gondolatot tovább fűzve megállapítható, hogy a kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftverek, internet,GPS,stb.) [8] A kritikus információs infrastruktúrák védelme tehát a tulajdonosok, gyártók, és használók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat. [8] Az információs stabilitás elérésének érdekében komplex információbiztonsági elveket kell alkalmazni. Ezeket a komplex és integrált védelmi intézkedéseket tudati, információs és fizikai dimenziókban is érvényesíteni kell a kritikus információk védelmének érdekében. Ezzel összefüggésben elmondható, hogy ezen a területen a minősített adat védelméről szóló 2009. évi CLV. Törvény (a továbbiakban: MAV törvény) már egységes irányelveket szab. A MAV törvény nyomán, a Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésének rendjéről szóló 90/2010.(III.26.) Kormányrendelet, és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet, viszont már egységes alapokra helyezi a minősített adatok védelme érdekében érvényesítendő, személyi, fizikai, dokumentum és elektronikai védelem komplex rendszerét.[10] Az elektronikai védelmi intézkedések keretei között megjelenik az átvitel út védelme, számítógép (szoftver, hardver és hálózat) védelme. [11] Egységesítésre kerültek a rejtjelzéssel összefüggő követelmények és megjelennek a kompromittáló kisugárzással kapcsolatos alapvető irányelvek. Sajnos a kompromittáló kisugárzás védelmének részletes szabályozását illetően megállapítható, hogy a magas színvonalú védelmi intézkedésekkel összefüggő

követelményrendszert nem sikerült érvényesíteni. Ennek az is lehet az oka, hogy – ez a viszonylag új és bonyolult terület – a leg költségigényesebb védelmi intézkedések megvalósítását feltételezi és ezen a területen hazai tapasztalatok hiányában a nemzetközi irányelvekre figyelemmel kell kialakítani a hazai szabályozást! Ezen a területen, az irányadó hazai információvédelmi szakemberek bevonásával, további lépések szükségesek ahhoz, hogy az elektronikai védelem területén a maradvány kockázatot optimalizáljuk és növeljük az elektronikai rendszerek egyenszilárdságát. Az viszont egyértelmű eredménye a fenti törvényben és kormányrendeletekben megfogalmazott szabályrendszernek, hogy a minősített adat védelmével összefüggő komplex védelmi intézkedések többé kevésbé koherensek lettek a nemzetközi szabályokkal, ennek okán az Európai Uniós és a NATO rendszereken belüli információáramlás (bizonyos szintig) egységessé és lehetővé vált!



3. ábra: A biztonsági dimenziók és az információbiztonság kapcsolata

3. AZ ORSZÁGOS TÁVKÖZLŐ HÁLÓZAT (OTH) FELHASZNÁLÁSA A VÉDELMI FELADATOKKAL ÖSZEFÜGGÉSBEN

Annak érdekében, hogy a rendszerben keletkezett kritikus információk kellően támogassák a döntési helyzetben lévő felelős vezetőket, az információ továbbítására alkalmas és képes nemzeti Országos kommunikációs távközlési hálózat magas szintű rendelkezésre állását kell biztosítani. Meg kell határozni a szükséges és elégséges szolgáltatás mértékét. Ennek előfeltétele a megfelelő szintű és tartalmú törvényi szabályozás, amely lehetővé teszi ezt a rendelkezésre állást a bonyolult nemzetközi tulajdonosi rendszer esetén is. Különösen fontos abban az esetben jól szabályozni ezt a területet, amikor például a védelmi szektor zártcélú vezeték nélküli kommunikációját biztosító rendszer szolgáltatója egy olyan egyetemes szolgáltató, amely külföldi tulajdonosi rendszerben üzleti alapokon szolgáltat. Ezt a részterületet hivatott szabályozni a Miniszterelnöki Hivatalt vezető miniszter 4/2010. (III. 26.) MeHVM rendelete a védelmi feladatokban részt vevő elektronikus hírközlési szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról.

Az elektronikus hírközlésről szóló 2003. évi C. törvény 182. § (4) bekezdés l) pontjában kapott felhatalmazás alapján a Miniszterelnöki Hivatalt vezető miniszter feladat- és hatásköréről szóló 29/2008. (II. 19.) Korm. rendelet 1. § j) pontjában meghatározott feladatkörében eljárva, a miniszterelnöki hivatalt vezető miniszter az alábbiakat rendelte el [12]:

Az elektronikus hírközlés szolgáltatási tevékenységének a minősített időszakban történő ellátásához szükséges védelmi felkészülési feladatok előkészítésében és végrehajtásában való részvételre kijelölt, valamint az informatikai és elektronikus hírközlési, továbbá postai ágazat (a továbbiakban: ágazat) ügyeleti rendszerébe bevont elektronikus hírközlési tevékenységet végző szervezetek (a továbbiak ban: szolgáltatók) felsorolását a rendelet 1. melléklete tartalmazza.

A riasztási és tájékoztatási feladat ellátásában részt vevő nem közszolgálati műsort sugárzó országos, körzeti, helyi rádió és televízióadók, az adókat üzemeltetők (engedélyesek) jegyzékét a rendelet 2. melléklete tartalmazza.

A kijelölés alapján a szolgáltatók a tevékenységi körüket érintően ellátják a minősített időszakban bekövetkező rendkívüli események megelőzésére, elhárítására, a következményeik csökkentésére, illetve megszüntetésére, valamint a helyreállításra irányuló védelmi felkészülési és végrehajtási feladatokat.

A rendelet alkalmazásában minősített időszak a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény 19. §-a (3) bekezdésének h) pontjában meghatározott rendkívüli állapot és i) pontjában meghatározott szükségállapot, az Alkotmány 35. § (1) bekezdésének i) pontja és a polgári védelemről szóló 1996. évi XXXVII. törvény 2. § (2) bekezdése szerinti veszélyhelyzet, valamint az Alkotmány 19. § (3) bekezdés n) pontjában meghatározott megelőző védelmi helyzet, továbbá a 19/E. § (1) bekezdésében foglalt, a szükségállapot vagy a rendkívüli állapot kihirdetésére vonatkozó döntésig terjedő időszak.

Az elektronikus hírközlésért felelős miniszter (a továbbiakban: Miniszter), illetve a Nemzeti Hírközlési Hatóság (a továbbiakban: NHH) a védelmi felkészülés és a végrehajtás időszakában felmerülő egyedi védelmi feladatokat az érintett szolgáltatók számára külön jogszabály szerint határozza meg.

A védelmi felkészülési feladatok végrehajtásáért minden esetben a szolgáltató vezető tisztségviselője felelős.

A szolgáltatók – a minősített időszakra történő felkészülés keretében – az alábbiakban meghatározott tevékenységi körökből a saját szervezetük szakmai feladat- és hatáskörébe tartozó védelmi feladatokat látják el:

- a szervezeti készenlét előkészítésének és fenntartásának körében:
  - a védelmi felkészülési feladatok ellátásához szükséges személyi, szervezeti és anyagi-technikai feltételek megteremtése, folyamatos biztosítása.
- a védelmi felkészüléssel, műszaki, forgalmi, katasztrófa vagy egyéb veszély miatt keletkező üzemzavar elhárításával kapcsolatos intézkedések kidolgozása, tervek készítése és azok folyamatos aktualizálása:
  - a védelmi felkészüléssel összefüggő rendszeres képzési, továbbképzési és gyakoroltatási feladatok meghatározása és végrehajtása;
  - az ügyeleti szolgálatnak a külön jogszabályban foglaltak szerinti működtetése;
  - a külön jogszabály alapján a meghagyással kapcsolatos feladatok végrehajtása.
- a hálózatok felkészítésének és irányításának terén:
  - a gerinchálózati struktúra és az elektronikus hírközlési létesítmények védelmi, biztonsági feltételeinek biztosítása;
  - a zártcélú hálózatokhoz szükséges összeköttetések és kapcsolódó szolgáltatások előkészítésének és alkalmazásának biztosítása;
  - a meghatározó szerepű elektronikus hírközlési csomópontok, illetve felhasználók több útvonalon történő elérhetőségét segítő megoldások kialakítása;
  - a riasztási és tájékoztatási feladat ellátására létrehozott rendszerben szükséges elektronikus hírközlési összeköttetések biztosításában való közreműködés;

  - be) a honvédségi, kormányzati, rendvédelmi elektronikus hírközlési eszközöknek a szolgáltató hálózatához történő csatlakoztatásához szükséges hozzáférési pontok és jogosultságok biztosítása.
- az üzemviteli és tartalékolási rendszer kialakítása terén:
  - a nemzeti és a nemzetközi gerinchálózati irányító és üzemviteli funkciók működésének összehangolása;
  - az illetékes hazai, valamint nemzetközi szervek és szervezetek közötti védelmi jellegű kapcsolattartás feltételeinek kialakításában és végrehajtásában való közreműködés;
  - az elektronikus hírközlési szolgáltatások területén elrendelhető korlátozó vagy szüneteltető rendelkezések végrehajtására és következményeik kezelésére történő felkészülés;
  - a védelmi feladatok ellátásához szükséges mértékű és összetételű tartalékkészletek biztosítása;
  - a hálózati létesítmények és eszközök meghibásodása, rongálódása, sérülése, megsemmisülése esetére az elsődleges helyreállításhoz és az üzemszerű állapot visszaállításához szükséges feladatok megtervezése és végrehajtási feltételeinek folyamatos biztosítása.
- a szolgáltatási igények kielégítése terén:
  - a védelmi felkészülésben részt vevő, külön jogszabályban meghatározott követelménytámasztó szervek minősített időszakra vonatkozó szolgáltatási igényeinek kielégítéséhez szükséges feltételek biztosítása, az összefüggő tervezési, szervezési tevékenység ellátása, szolgáltatási feladatok végrehajtása;
  - a lakosság minősített időszaki elektronikus hírközlési igényeinek az egyetemes szolgáltatási, illetve koncessziós szerződésben meghatározott szinten és tartalommal történő kielégítéséhez szükséges feltételek biztosítása;
  - a védelmi felkészüléssel kapcsolatos jogszabályok által meghatározott gazdasági és anyagi szolgáltatási kötelezettségek teljesítésére, illetve kezelésére való felkészülés;
  - da kormányzat minősített időszaki szolgáltatási igényeinek kielégítéséhez és kommunikációs tevékenységéhez szükséges feltételek megteremtésében, fenntartásában való közreműködés;
  - a Befogadó Nemzeti Támogatás tervezési és végrehajtási feladataiban történő részvétel.
- a nyilvántartások vezetése és az adatkezelés terén:
  - a védelmi felkészülési feladatokkal kapcsolatos jogszabályokban meghatározott adatszolgáltatási kötelezettség teljesítéséhez szükséges nyilvántartási rendszer kialakítása és adatainak a követelményekhez igazodó pontosságú karbantartása.
- a műsorszórási tevékenység körében:
  - a műsorszórási tevékenység folyamatosságához szükséges technikai és biztonsági feltételek megteremtése, a meghatározó szerepű létesítmények őrzés-védelmének biztosítása;
  - a műsorszóró hálózaton a lakosság légi-, illetve katasztrófariasztásra és tájékoztatására létrehozott rendszer működésében való közreműködés;
  - a lakosság légi-, illetve katasztrófariasztásának és tájékoztatásának elrendelésére illetékes szervek intézkedésére a riasztási és tájékoztatási közlemények leadásának – az elrendelő szervekkel kötött megállapodás szerinti, saját eszközökkel történő – biztosítása.

A riasztási és tájékoztatási feladat ellátásában külön jogszabály alapján – az illetékes honvédelmi és rendvédelmi szervek, valamint a közszolgálati rádió és televízió

műsorszolgáltatók, műsorszóró adók és az adókat üzemeltető szolgáltatók mellett – részt vesznek:

- a Miniszter és az NHH;
- a rendelet 2. mellékletében meghatározott nem közszolgálati országos, körzeti és helyi rádió és televízió műsorokat sugárzó adók, az adókat üzemeltetők (engedélyesek);
- azok az elektronikus hírközlési szolgáltatók, amelyek összeköttetést, illetőleg modulációs vonalat biztosítanak:
  - a riasztási és tájékoztatási közlemény leadását kezdeményező szerv és az érintett rádió, televízió stúdiója között;
  - a riasztási és tájékoztatási feladatban részt vevő stúdió és a részére sugárzást végző rádió, televízió adóállomás között, valamint;
  - a műsorszolgáltatók és a műsorszóró adók között.
- a riasztási rendszer technikai elemeit, a riasztási és tájékoztatási közlemények átvételére és továbbítására szolgáló átkapcsoló berendezések fenntartását ellátó gazdálkodó szervezet.

4. AZ EURÓPAI UNIÓ LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK FIGYELMEZTETŐ ÉS INFORMÁCIÓS HÁLÓZATA (CIWIN)

4.1. Vezetés irányítási rendszerek alapvető megközelítése

Az információbiztonsági stabilitást alapvetően befolyásoló OTH, magas szintű rendelkezésre állása és a minősített adatok védelmével összefüggő részterületeken túl, az alábbiakban célszerű megvizsgálni a globális, nemzetközi, nemzeti és regionális infokommunikációs rendszerekre épülő vezetés-irányítási rendszerekkel összefüggő alapvető ismereteket és követelményeket. Ennek nyomán célszerű áttekinteni - egy a kritikus infrastruktúra védelmével összefüggő- adattovábbítási értesítési és riasztási rendszerrel szembeni alapvető igényeket is. Különösen indokolt ez, annak fényében, hogy az összekapcsolódó (adott esetben globális) infrastruktúrákon keresztül – az incidens bekövetkezését követően- a működési zavarok felhalmozódnak, hatványozódnak az interdependencia jelenség miatt. Ebben a helyzetben indokolt egy nemzetközi (európai) adatok cseréjére alkalmas megosztott figyelmeztető és tájékoztató rendszer alkalmazása, amelynek segítségével a döntéshozók, az egységes és valós idejű adatok alapján rövid idő alatt a helyzettel összefüggő széleskörű adatszolgáltatás alapján képesek meghozni az optimális döntéseket. Az információs társadalomban alapvető igény fogalmazódik meg az infokommunikációs eszközökre épülő valós idejű globális döntés támogató rendszerek üzemeltetésére. Ezzel összefüggően megállapítható, hogy a kritikus infrastruktúra védelem területén is alapvető igény az információs fölény birtoklása, annak érdekében, hogy a fenyegetések előrejelzése, majd annak realizálódását követően a kár elhárítás és a működőképesség helyreállításának időszakában is optimális szinten tartható legyen a szükséges és elégséges szintű védelmi intézkedések alkalmazása.

4.2. A CIVIN kezdeményezés bemutatása

A CIWIN létrehozására irányuló kezdeményezések már 2006 decemberére nyúlnak vissza. A létfontosságú infrastruktúra védelem Európai Programja (EPCIP) javaslatok célkitűzések értelmében fogalmazódott meg egy az infrastruktúra védelemmel összefüggő, biztonságos információcserére alkalmas eljárás kidolgozása. Ez a kezdeti lépés alapozta meg egy tagállamok közötti kölcsönös tájékoztató rendszer létrejöttét, illetve fogalmazta meg annak igényét. Erről az Európai Bizottság határozatban is gondoskodott ugyan, de a tagállamok

CIWIN- hez történő csatlakozása nem kötelező. Ugyanakkor az EPCIP-vel kapcsolatos irányelveknek megfelelően a tagállamoknak az Európai Bizottság részéről rendelkezésre bocsátott információkat hozzáférhetővé kell tenniük a kijelölt ágazatok részére. A tagállamoknak viszont a saját területéről gyűjtenie kell az adatokat az európai létfontosságú infrastruktúrákról, a sebezhetőségi és függőségi pontjairól, a védelmi fejlesztésekről és ezt elérhetővé kell tenni az EU részére.

A CIWIN (szerver / kliens) rendszer funkcionalitását illetően, a Bizottság és a tagállamok közötti viszonylatban alkalmasnak kell lennie a két vagy többoldalú információ megosztásra, illetve gyors riasztási funkció megvalósítására. A bizottsági felületen az ágazati területek jelennek meg. A rendszer kötött és dinamikus területi adatkezelésre egyaránt alkalmas.

A kötött területen jelennek meg a tagállami, szektor, vezetői, külső együttműködési területek és egy gyors információcserét biztosító RAS alrendszer.

Egy speciális esemény, vagy tagállami projektek, szakértői munkacsoport terület részésze, igény szerint dinamikus területek hozhatók létre.

Az elrendelt figyelmeztetés esetén lehetőség van egy ideiglenes RAS terület létrehozására, amely az együttműködés színtere az adott projektre vonatkozóan.

A kritikus infrastruktúra védelmével összefüggő és rejtelzéssel védeni rendelt, minősített információk megosztására speciális terület áll rendelkezésre azok számára, akik a „muszáj tudni” elv alapján azokhoz jogosultak hozzáférni.

A CIWIN rendszer (MS SharePoint 2007), piaci alkalmazásra épül és beépített, minden nyelvre automatikus fordítóprogramot, illetve „off the shelf” tartalomkezelőt használ. Funkcióit illetően megtalálhatóak benne a vitafórum, kalendárium, és a személyes belső levelező funkciók is.

A TESTA rendszeren történő elérést megelőzően, minősített információk továbbítására nem alkalmas. Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de közép távon -sTESTA hálózaton- Bizalmas minősítésű információk megosztására lesz alkalmas.

A TESTA (Trans European Services for Telematics between Administrations) egy független zártcélú (publikus hálózatoktól független) gerinchálózat, amely az Európai Unió adminisztrációja és a tagállamok közötti kommunikációs hálózat. A TESTA rendszer, információvédelmi szempontból továbbfejlesztett változata az sTESTA, amely már megfelelő egyenszilárdságú rejtjelző eszközöket és algoritmusokat használ. A tagállamok részére a CIWIN rendszerre történő csatlakozás opcionális, azonban a rendszerhez csatlakozó tagállamoknak a minősített adatkezeléssel összefüggő kötelezettség alapján az elektronikai, dokumentum, személyi és fizikai védelmi követelményeknek meg kell felelni. Az előzőekben már kifejtett EU minősített adatvédelmi követelményekkel koherens szabályozási rendszer, különösen ezen a területen nyit új távlatokat, melyeket az Európai Bizottság, a tagállamokkal kötött többoldalú szerződésekkel is megalapozott.

Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de közép távon Bizalmas minősítésű információk megosztására lesz alkalmas.

4.3. Információvédelmi kérdések

Az Európai Bizottság által kiadott irányelv 9. cikkelyében megfogalmazottaknak megfelelően., a minősített információt kezelő személyeknek, személyi biztonsági tanúsítvánnyal kell rendelkezniük. Ennek előfeltétele a megfelelő szintű nemzetbiztonsági átvizsgálást követő kockázatmentesség megállapítása. A tagállamoknak, a Bizottságnak és az illetékes felügyeleti szerveknek (ez hazánkban a Nemzeti Biztonsági Felügyelet) biztosítaniuk kell, hogy a minősítet információkhoz a létfontosságú infrastruktúrák védelme céljából jussanak hozzá, az arra jogosult személyek. Ezzel összefüggésben elengedhetetlen a nemzeti és nemzetközi jog harmonizációja (ez meg is történt) valamint az egységes jogértelmezésen alapuló jogkövető magatartás érvényesítése. Az egyes tagállamoknak és a

bizottságnak egyaránt tiszteletben kell tartania a minősített adat minősítője által megállapított minősítési szintet.

A CIWIN rendszer információs funkciója biztosítja, hogy az adathoz való hozzáférés alapja a már említett"tudnia kell" elv alkalmazása. A rendszeren belül az információ birtokosa dönti el azt, hogy ki és milyen biztonsági szinten férhet hozzá az adathoz. A tagállamok jogosultsága és felelőssége az, hogy tagállamon belül hogyan szabályozzák a hozzáférést az adathoz. Természetesen itt vissza kell utalni a koherens EU és nemzeti szabályokra, melynek rendelkezéseit maradéktalanul be kell tartani. A tagállamnak minden alkalommal ki kell jelölnie egy arra jogosult vezetőt, aki a jogosultságokat illetően dönteni tud. Ez az egyszemélyi vezető jogosult ezeket a jogokat – korlátozott mértékben- a tagállam más tisztségviselőjére delegálni. A szabályoknak megfelelő szintű személyi biztonsági tanúsítványokkal a kezelőknek és felhasználóknak egyaránt rendelkezniük kell.

4.4. Hazai rendszerek együttműködése a CIWIN rendszerrel

A nemzeti KIV hatókörében, az irányadó szakemberek szerint nem szükséges külön riasztási és értesítési rendszereket létrehozni. Azt azonban célszerű elemezni, hogy a jelenleg működő riasztási és értesítési rendszerek, hogyan tudják támogatni a nemzeti KIV-ben érintett szektorok és az állami szektor döntésképes vezetőit. Ha a vizsgálat eredménye ként erre a jelenlegi rendszerek nem alkalmasak, akkor (és csak is akkor) szükséges új, különálló rendszerek fejlesztésében gondolkodni. Ugyanakkor védelmi vezetéstechnikai rendszerszervezési szempontokat figyelembe véve, nem indokolt sok sziget rendszerű riasztási rendszert üzemeltetni. Célszerű a jövőben megvizsgálni annak a lehetőségét is, hogy a meglévő nemzeti rendszereket (Marathon Terra; K-600/KTIR) illetve azok bizonyos adatbázisait (amelyek nem sértenek nemzeti érdekeket) egy funkcionális interfészen keresztül, hogyan lehet elérhetővé tenni a CIWIN számára, egységes és redundáns platformra helyezve ezzel a nemzeti és európai KIV figyelmeztető és információs rendszereit.

ÖSSZEFOGLALÁS

A biztonság újkori értelmezéséből kiindulva - elfogadva azt, hogy a dimenziók átalakultak és némely dimenziók felértékelődtek – megállapítható, hogy az információs társadalom kritikus infrastruktúrának és ezen belül a kritikus információs infrastruktúra védelmével összefüggő kérdések a biztonsági stratégiába épülő és annak szerves részét képező elemei. Megállapítható, hogy a társadalom zavartalan működésén túl, a katasztrófa helyzetben és a különböző minősített időszaki helyzetekben súlyponti kérdés a kritikus információs infrastruktúrák rendelkezésre állása. Az mára bizonyított tény, hogy az információk gyors, hiteles és változatlan formában történő áramlása alapvetően befolyásolja a védelmi intézkedések hatékonyságát. A fentiekből azt a végkövetkeztetést lehet levonni, hogy ezen a területen is fontos az információs fölény elérése.

A külföldi és hazai jogi és technológiai környezetet elemezve az a végkövetkeztetés vonható le, hogy a hazai szabályozás – a hazai doktrínák rendszerét vizsgálva – ugyan igyekszik követni az európai folyamatokat, de különösen technológiai területen az útkeresés fázisában lévő folyamat érzékelhető. A felhasználók igénye az információs rendszerek használatával kapcsolatban nagyon határozott és jól érzékelhető, de különösen az érzékeny, vagy minősített adatok gyors, hiteles és változatlan továbbítására alkalmas hazai rendszerek kialakítása még várat magára. Ezen a területen több párhuzamos fejlesztési folyamat érzékelhető. Ezért is különösen fontos annak a problémának a feloldása, hogy a hazai és nemzetközi értesítési rendszerek egységes platformon és egységes elvek alapján képesek legyenek a hatékony együttműködésre. A fentieket összefoglalva, irányadó szakemberek szerint az információs társadalom zavartalan működését veszélyeztető fenyegetésekkel

szembeni védelmi intézkedések foganatosítása az információs dimenzióban, meghatározó szerepet töltenek be.

HIVATKOZÁSOK

[1] Egyesült Nemzetek Nevelésügyi és Kulturális Szervezete (UNESCO) társadalomtudományi szótár

[2] Amerikai nemzetbiztonság c. könyv (1981)

[3] A Magyar Köztársaság nemzeti Biztonsági Stratégiájáról szóló 2073/2004.(IV.15) korm. határozat.

[4] Kőszegvári Tibor: A hadtudomány mai problémái, területei és új fogalma (Hadtudomány, Magyar Hadtudományi Társaság, Budapest XVII. évfolyam 2007/1. szám) 13. oldal

[5] Farkasné dr. Zádeczky Ibolya: A biztonságot veszélyeztető globális kihívások (Hadtudomány, MHTT. Budapest XVI. évfolyam 3. szám, 2006. szeptember) 41. oldal.

[6] Wörterbch zur sicherheitspolitik, Mitter Kiadó, 1985. 113. o.

[7] Szabó József: Hadtudományi Lexikon, Magyar Hadtudományi Társaság, 1995. 144. o.

[8] Muha Lajos: A Magyar Köztársaság Kritikus Információs Infrastruktúráinak védelme doktori (Phd) értekezés 2007.

[9] A minősített adat védelméről szóló 2009. évi CLV. Törvény

[10] A Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésének rendjéről szóló 90/2010.(III.26.) Kormányrendelet

[11] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet

[12] Az elektronikus hírközlésről szóló 2003. évi C. törvény

Farkas Tibor – Pándi Erik – Töreki Ákos – Hóka Miklós
farkas.tibor@zmne.hu – pandi.erik@zmne.hu – toreki.akos@zmne.hu – hoka.miklos@zmne.hu

A NATO VEZETÉSŰ TÖBBNEMZETI MŰVELETEK HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSA[1]

Absztrakt

Jelen közlemény a magyar haderő missziós tevékenysége híradó és informatikai támogatásának kérdését tárgyalja.

This publication deals with the question of Communication and IT support provided for mission operations of the Hungarian Army.

Kulcsszavak: *Magyar Honvédség, NATO, híradó és informatikai támogatás ~ Hungarian Defence Forces, NATO, IT support*

BEVEZETÉS

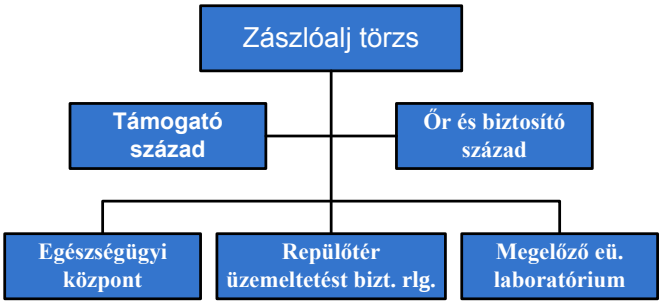
A világ jelenlegi biztonságpolitikai kihívásai és a nemzeti érdekek megkövetelik, hogy a szövetségek tagállamai összefogva, hatékonyan reagáljanak a megjelenő kockázatokra, fenyegetésekre. A különböző missziós műveletek során a magyar haderő távoli helyeken lát el feladatokat a globális béke és biztonság megteremtéséhez és fenntartásához, a terrorizmus és más, új típusú fenyegetések elleni tevékenységek katonai feladatainak végrehajtása érdekében. Magyarországhoz legközelebb elhelyezkedő, ezért számunkra kiemelten fontos válságövezet a Balkán. A Koszovóban tevékenykedő, a NATO parancsnoksága alatt működő nemzetközi békefenntartó haderő (KFOR: Kosovo Force) missziós tevékenysége mellett számos magyar katona (tiszt, tiszthelyettes) szolgál különböző NATO parancsnokságokon. A balkáni magyar szerepvállalás jelentősége és kiemelt fontossága napjainkban is töretlen. Katonáink jelen vannak a Balkánon, a Közel-Keleten, illetve Afrika válságövezeteiben – magyar alegységek tagjaként, vagy egyedi beosztásokban –, és az ott folytatott sikeres részvételünk bizonyítja, hogy a magyar haderő képes a nemzeti- és a nemzetközi érdekeket képviselni határainkon kívül.

1. A MAGYAR HONVÉDSÉG ŐR- ÉS BIZTOSÍTÓ ZÁSZLÓALJ HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSA

A KFOR misszió 1999-es megalakulását követően, a Magyar Köztársaság egy zászlóalj szintű erővel járult hozzá a térség rendezését célzó erőfeszítésekben való részvételhez. Az 55/1999 OGY határozatban került meghatározásra a Magyar Honvédség Őr- és Biztosító Zászlóalj (MH ŐBZ) felállítása és annak maximális létszáma. „Az Országgyűlés figyelemmel […] a Magyar Köztársaság a koszovói békefenntartásban részt vevő nemzetközi erőkhöz (KFOR) a feladataihoz szükséges fegyverzettel, technikai eszközökkel, felszereléssel és logisztikai támogatással ellátott, őr- és biztosítási feladatokat végző zászlóaljjal járuljon hozzá. A zászlóalj létszáma nem lehet több, mint 350 fő, amely a váltási periódusokban sem haladhatja meg az 500 főt.” [1]

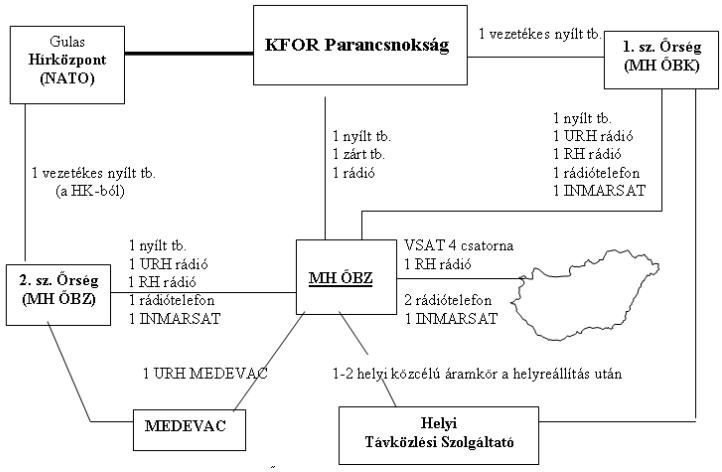
1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

A zászlóalj a koszovói Pristina területén található „Szent László táborban” települt. Feladatai közé tartozott a „Film City”[2], a magyar tábor, és a „Vrelo” tábor őrzés-védelme, „fontos személyek” (VIP: Very Important Person)- és szállítmányok kísérése, rendezvénybiztosítás, járőrözés, mobil ellenőrző áteresztő pontok (EÁP)[3]-ok telepítése, működtetése.



1. ábra: Az Őr- és Biztosító Zászlóalj felépítése

A feladatok híradó biztosítása széleskörű technikai eszközök használatát követelte meg, mivel mind az őrzésvédelem, mind a szállítmánykísérés más és más híradó-technikai eszközöket igényel. Az MH ŐBZ híradó és informatikai biztosításának megszervezéséért a Honvéd Vezérkar (HVK) híradó csoportfőnök, az operatív irányításért pedig az MH Szárazföldi Parancsnokság (MH SZFP)[4] Vezetési Főnökség Kiemelt Híradó Főtiszt volt a felelős. A zászlóalj a KFOR parancsnokság hadműveleti és az MH SZFP szolgálati alárendeltsége alatt hajtotta végre a feladatait.



2. ábra: Az Őr- és Biztosító Zászlóalj hadműveleti híradás vázlata
Forrás: [2]

2 A KFOR parancsnokság területének megnevezése.
3 Egy speciális katonai elem, amely meghatározott helyen kerül telepítésre az áthaladó gyalogos- és járműforgalom ellenőrzése, szállítmányok átvizsgálása céljából.
4 Az MH Szárazföldi Vezérkar 2001-ben alakult át Szárazföldi Parancsnoksággá. Az MH ÖBZ 2007-ig az SZFP irányítása alatt hajtotta végre feladatait.

1.1. A zászlóalj és az elöljárók között szervezett híradás

Az MH ŐBZ „vezetési pontján”, Pristinában települt a híradó- és informatikai központ. A központból VSAT[5] műholdas összeköttetés került kialakításra Magyarország irányába távbeszélő csatornákon, amelyek Budapesten kerültek csatlakoztatásra az MH távhívó hálózatába. „A VSAT rendszerek elsősorban a magasabb vezetési szintek irányítási, valamint belföldi és nemzetközi együttműködési híradásában alkalmazhatók, […].” [4] A VSAT kapcsolat itt került elsőként alkalmazásara a Magyar Honvédség részéről, amely tartalékaként Inmarsat[6] műholdas híradást szerveztek a nemzeti elöljáró irányában történő kapcsolattartás céljából. Az Inmarsat nyílt hang-, fax- és adatátvitelt biztosít, amely a VSAT csatorna távfelügyeleti átviteli útja is egyaránt. Az MH Őr- és Biztosító Zászlóalj alkalmazott elsőként Inmarsat mini-M műholdas eszközöket. Az első Inmarsat alkalmazásra Okucaniban került sor, ahol az MH Magyar Műszaki Kontingens Inmarsat–M készülékeket használt fel a kommunikáció megvalósítására, amely hang-, fax-, és adatkommunikációt biztosított.

A zászlóalj másodlagos kapcsolattartási lehetősége Magyarországgal HARRIS RF-5200 rádió felhasználásával került megszervezésre, amely az amerikai hadseregtől segélyként kapott rádiókból került ki. Ez a készüléktípus kiválóan alkalmas a nagytávolságú összeköttetés megvalósítására, azonban nem volt hivatalosan rendszerbe állítva. A mai missziós feladatok ellátása során az újabb generációs Harris rádiók (FALCON II., III.) esetében ez a probléma megoldódott, a szervízelés és a pótalkatrészek biztosítottak. A megszervezett rövidhullámú rádióháló titkosítása biztosított volt az eszközbe szerelt titkosító modullal[7], így az minősített közlemények továbbítását is biztosította.

Az „anyaország” irányába továbbá mobiltelefonos (GSM: Global System for Mobile Communications) összeköttetés is rendelkezésre állt, a felszerelési jegyzékben szereplő, a zászlóalj részére kiadott hazai SIM (Subscriber Identity Module) kártyás mobiltelefonokkal.

Az alegység hadműveleti parancsnoksága, a KFOR parancsnokság irányában 1-1db nyílt- és zárt távbeszélő, illetve 1db rádió összeköttetés került megszervezésre. A híradó vonalat az elöljáró híradó- és informatikai főnöke szervezte és tervezte. Az összeköttetés megvalósítása, a vezetékek kiépítése érdekében az elöljáró irányalegységet telepített a kontingenshez. A rádiós összeköttetés frekvencia-kiutalására szintén az elöljáró intézkedett.

1.2. A zászlóalj hadműveleti híradása

A kontingens hadműveleti híradása összetett, többszintű összeköttetéseket foglalt magába, melyeknek egy részét az elöljáró biztosította, másik részét az alegység híradó- és informatikai főnöke szervezte, tervezte. Az összeköttetés az alábbi legfontosabb területekre terjedt ki:

- a kontingens (tábor) belső híradása;
- a zászlóaljparancsnokság és a kihelyezett őralegységek, valamint az őralegységek és a KFOR Parancsnokság közötti összeköttetések;
- a kihelyezett őralegységek belső híradása;
- a konvojok, és az esetleges kirakóhelyek rádióhíradása;
- és az egészségügyi (légi) mentés (MEDEVAC: Medical Evacuation) híradása.

5 „Definíció szerint a VSAT (Very Small Aperture Terminal - Nagyon Kis Átmérőjű Antennával Működő Terminál) rövidítés olyan kisméretű (kb. 0,5-3,5 m átmérőjű) antennával rendelkező űrtávközlési földi állomást jelent, amely könnyen, gyorsan telepíthető rendeltetési helyére. A VSAT-okkal felépült távközlési hálózat általában "csillag" elrendezésű.” [3]

6 International Maritime Satellite: Nemzetközi tengerészeti műholdas rendszer, amely mozgó- és állandó telepítésű távközlési összeköttetésekre egyaránt alkalmas.

7 Az MH Központi Rejtjelfelügyelet intézkedése alapján történ meg a kulcsellátás.

Az elöljáró biztosította az őralegységek vezetékes híradását a zászlóaljparancsnokság és az őrparancsnokok között 1db nyílt távbeszélő vonallal. A híradó- és informatikai főnök (HIRIF) feladata volt biztosítani a tábor belső híradását az őralegységek belső vezetékes híradását, az alegységek belső híradását, és a konvojok menthíradását rádióforgalmi rendszerek kialakításával a rendelkezésre álló eszközökkel. Fontos megemlíteni a helyi vezetékes kommunikációs szolgáltatók által nyújtott lehetőségeket. A kezdeti nehézségeket követően, a kontingens helyi vezetékes vonalakat bérelt, amellyel biztosítva volt a helyi, koszovói közigazgatási szervekkel való együttműködés. A helyi GSM szolgáltatók rendszerét szintén fel lehetett használni.

A HIRIF számára különös figyelmet kellett fordítani a MEDEVAC biztosítására. A részlegeket, konvojokat el kellett látni URH rádiókészülékekkel, MEDEVAC forgalmi adatokkal, és fel kellett készíteni a katonákat az előírásoknak megfelelő segélykérés leadására.

Az MH ŐBZ állománya magánbeszélgetésének biztosítása érdekében 3 db kihelyezett mellék állt rendelkezésre, amelyeken a katonák Magyarország irányába folytathattak telefonbeszélgetéseket. Természetesen ezek „R” beszélgetések lebonyolítására voltak alkalmasak.

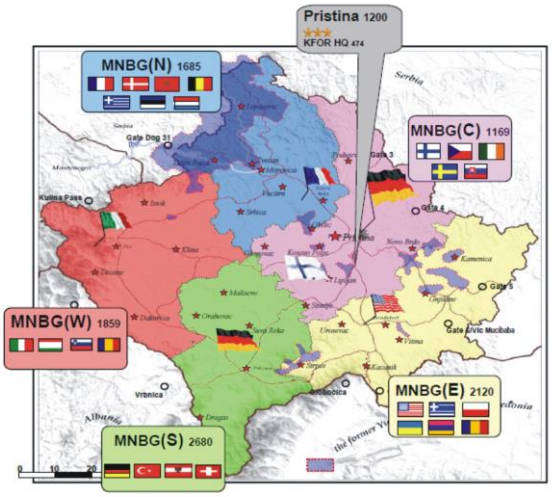
Az MH ŐBZ mint ideiglenesen létrehozott szervezet megszüntetéséről az MH 97/2008. (HK 13) HM határozatban[8] rendelkeztek.

2. A KFOR ZÁSZLÓALJ HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSA

Az MH ŐBZ a 18. váltását követően megszűnt, majd a megújult feladatok ellátása érdekében egy új szervezet jött létre, az MH KFOR Zászlóalj (KFOR Z). Az új alegység önálló felelősségi területtel rendelkező többnemzeti zászlóalj. A kontingens két szlovén századdal egészült ki, a vezető szerepet a nemzetek felváltva töltik be. Az új szervezet támaszpontja Koszovó nyugati részén, Pec városánál található.

A magyar zászlóalj a KFOR parancsnokság közvetett alárendeltségében hajtja végre a számára meghatározott tevékenységeket, feladatokat. A koszovói KFOR erőket öt többnemzeti kötelékbe (MNTF: Multinational Task Forces)[9] szervezték. Mind az öt MNTF saját működési területtel rendelkezik és a KFOR parancsnoknak vannak alárendelve. A működési területükön belül a biztonság szavatolása, határellenőrzés és egyéb helyreállítási munkák biztosítása, ellátása a fő feladat.

8 MH határozat a Magyar Honvédség Őr- és Biztosító Zászlóalj ideiglenes katonai szervezet megszüntetéséről. [6]
9 Későbbi megnevezése: Többnemzeti Alkalmi Harci Kötelék (MNBG: Multi National Battle Group).



3. ábra: A KFOR parancsnokságok és azok nemzeti összetétele
Forrás: [5]

Koszovó nyugati részének biztosítása a Nyugati Többnemzeti Kötelék (MNTF-W: Multinational Task Force West) feladata, amely a KFOR Zászlóalj műveleti elöljárója. Az MNTF-W feladata a régión belül ellenőrizni a nemzetközi egyezmények betartását, a közbiztonság fenntartását, és biztosítani a nemzetközi szervezetek munkáját. Az MNTF-W parancsnokság Pec városától körülbelül 20 km-re található, és a Villaggio Italia[10] táborban települt.

A KFOR Z 2008. szeptember 1-jén kezdte meg a feladatainak ellátását. Az ideiglenes katonai szervezet 450 fős létszámban lett maximalizálva. A zászlóalj híradásáról, informatikai támogatásáról és információvédelmének biztosításáról a HM Jogi Szakállamtitkár és a HM Honvéd Vezérkar Főnök együttes intézkedése rendelkezik. [7]

A KFOR Z az MH ÖHP szolgálati, és a külföldi alkalmazási körzetben a KFOR MNTF-W nyugati szektorparancsnokság parancsnokának műveleti irányítása alatt hajtja végre a meghatározott feladatokat. Rendeltetéséből adódóan - amely a KFOR műveleti területén történő békefenntartó feladatok ellátása - objektumvédelemi; területbiztosítási; területzárási; ellenőrzési; konvoj-, VIP kisérési; tömegkezelési; fegyverbegyűjtési feladatokat lát el. Ellenőrző-áteresztő-, és megfigyelő pontok működtetése mellett járőrözési feladatokat is ellátnak a zászlóalj kijelölt részlegei, amelyek a területbiztosítási feladatok elemei. A zászlóalj feladatainak ellátása érdekében megbízható híradó- és informatikai rendszer került telepítésre, amely garantálja a különböző típusú műveletek végrehajtását, és a parancsnok és törzse részére a vezetés és irányítás híradó támogatását. A megszervezésre került hírrendszer biztosítja az összeköttetést az elöljárókkal, hadműveleti feladatteljesítés esetén az alárendeltekkel. A kontingens híradó- és informatikai támogatását e két területre történő bontásával kívánjuk megvizsgálni.

2.1. A KFOR Zászlóalj híradása az elöljáróval

A zászlóalj a nemzeti elöljáró parancsnokságokkal történő kapcsolattartás kialakítása kiemelt fontosságú, mivel a tevékenységről folyamatos jelentést kell tennie az MH ÖHP irányába. A folytonos kapcsolattartás lehetővé teszi a tájékoztatás mellett az utánpótlások biztosítását is.

10 A tábor az „Olasz Falu” elnevezést kapta.

Magyarország és a zászlóalj közötti kapcsolat létesítéséhez szükséges híradó-technikai eszközök és a kapcsolódó szolgáltatások az elöljáró által biztosításra kerülnek.

Az elsődleges összeköttetési forma a VSAT műholdas kapcsolat, amely végberendezései az elöljáró által meghatározottak szerint kerülnek felprogramozásra. A telepített terminálokhoz kapcsolják azokat az eszközöket, amelyek a különböző szolgáltatásokat biztosítják. Ilyen lehetőség a távbeszélő központ csatlakoztatása a távbeszélő összeköttetés kialakításához. A tábor területén telepített műholdas végberendezések bérelt vonalon, bérelt szolgáltatás keretében kerülnek csatlakoztatásra az MH zártcélú távközlő hálózatába[11]. A szolgáltatás által biztosított sávszélességet a civil szolgáltató és a Magyar Honvédség közötti szerződés szabályozza.

A VSAT műholdas összeköttetés szolgál átviteli útként az informatikai szolgáltatások biztosítására is úgy, mint az Internet-, és Intranet[12] szolgáltatások. Bár a műholdas kapcsolatok kiemelten fontosak – elsődlegesek – a missziós feladatok ellátásánál, de használata igen költséges, amely körültekintő felhasználást követel meg. Ezt Sándor Miklós és Magyarné Kucsera Erika is kiemelte a zártcélú hálózat forgalmi optimalizálásának vizsgálatánál: „A nemzeti területen kívül tevékenykedő alegységeink híradásának jelentős része különböző típusú műholdas bérelt összekötetéseken keresztül valósul meg, melyek díjszabás szerinti bérleti- és forgalmi költsége jelentős, ezért az optimális forgalmi szituáció kialakítása jelentős költségmegtakarítást eredményez.” [9]. Az eszközök telepítését és üzemeltetését a jelölt kezelőállomány, a Híradó és Informatikai Konténer (HIK) kezelőszemélyzete végzi.

A VSAT összeköttetés tartalékaként Inmarsat műholdas berendezések kerülnek telepítésre, amelyek biztosítják az elöljáró irányába a kapcsolattartást. Az Inmarsat eszközök mellett Iridium[13] egyedi műholdas készülékek is felhasználásra kerülhetnek. Természetesen ezek kiegészítő eszközei, tartalékai az elsődleges összeköttetési formának, amelyek a műveleti feladatok híradó támogatására is alkalmazhatóak.

Az Inmarsat eszköz a VSAT kapcsolat és a rendszerfelügyelet tartalékaként üzemel, szükség esetén telefax eszköz is csatlakoztatható hozzá. Az Iridium megbízható összeköttetést nyújt, amelyen nyílt hangátvitel biztosított. Fő alkalmazási területe a kontingensvezetők szolgálati célú, és a funkcionális alegységek műveleti híradásának biztosítása.

Amennyiben a hadműveleti elöljáró rendelkezésre bocsát távbeszélő melléket a kontingens részére, amely rendelkezik NATO IVSN (Initial Voice Switched Network)[14] jogosultsággal, akkor az MH zártcélú távközlő hálózata elérhető IVSN hívással, amely a VSAT összeköttetés tartalékaként funkciónál. Magyarországra irányuló hívások kezdeményezhetők továbbá helyi szolgáltatótól bérelt közcélú hálózaton[15] keresztül, de ezek kizárólag a szolgálati feladatok ellátásával kapcsolatos hívások lehetnek. A kontingens az MH mellékkel nem rendelkező szervezetekkel való kapcsolatfelvétele ezen a rendszeren

11 Zártcélú hálózat: "Kizárólagosan kormányzati, nemzetbiztonsági, közbiztonsági és védelmi érdekeket szolgáló - rendeltetésük szerint elkülönült - távközlő hálózatok és berendezések, amelyek speciális igények kielégítését, zárt szervezet, illetőleg technika működését szolgálják. Használatuk (működtetésük) nem minősül távközlési szolgáltatásnak." [8]

12 Egy cég, szervezet saját belső hálózata, ahol a különböző Internet alapú szolgáltatásokat csak a belső számítógépekről lehet igénybe venni. A Magyar Honvédség belső hálózata az MH Intranet.

13 Globális mobil távközlési eszközök közötti kommunikáció megvalósítását biztosító rendszer.

14 Az IVSN egy korai, beszédkapcsolaton alapuló NATO hálózat, amely a beszédalapú szolgáltatásokat biztosítja. Ez volt az első NATO automata hang alapú hálózata. A kezdetben analóg technológián alapuló hálózat, amely elsősorban beszéd alapú kommunikációt biztosított, hasonló volt a polgári nyilvános kapcsolású hálózatokhoz (PSTN: Publich Switched Telephone Network), bizonyos katonai kiegészítésekkel.

15 „Közcélú (közhasználat céljára létrehozott) távbeszélő hálózat: Szolgáltatás-hozzáférési pontok, átviteli utak és ezek összekapcsolását végző kapcsolóberendezések együttese, amely lehetővé teszi, hogy bárki, aki - azonos feltételek mellett - igénybe kívánja venni, egy szolgáltatás-hozzáférési pontra csatlakoztatott végberendezés használatával egy másik szolgáltatás-hozzáférési pontra csatlakoztatott végberendezés használójával beszédkapcsolatot - illetőleg ennek jellemzőivel megegyező -, egyéb információátvitelt létesítsen.” [10]

keresztül valósul meg, de minden más összeköttetés kiesése esetén használható az elöljáróval való kapcsolattartás céljából.

A zászlóalj számára további hazai kapcsolattartási lehetőségként GSM telefonok kerültek kiosztásra, amelyek hazai telefonszolgáltató előfizetéses SIM kártyáival vannak ellátva. Ezek használata kizárólag kivételes esetekben engedélyezett, az egyéb kapcsolatok kiesése esetén. A mobiltelefonok felhasználása az országok közötti mozgás alatt engedélyezett, illetve külön parancsnoki engedély esetén feladat végrehajtás során, amennyiben más összeköttetésre nincs lehetőség. A helyi mobiltelefonokat hazai kapcsolattartásra csak indokolt esetben, a parancsnok szabályozásának megfelelően lehet felhasználni, lényegében tartalék eleme a hírrendszernek.

A hazai elöljáróval való kapcsolattartás további lehetősége a külön erre a célra szervezett rövidhullámú rádióforgalmi rendszer (RH rfr.), amely nem átszervezhető. A feladat ellátására RF-5200-as rövidhullámú rádiókészülék került kijelölésre, amely folyamatos ellenőrzése alapvető követelmény.

A hírrendszer futár- és tábori posta (FTP) híradását[16], a szolgálati-, nyílt- és magánküldemények továbbítását az MH 64. Boconádi Szabó József Logisztikai Ezred végzi. A futárszolgálatok indításának megszervezéséért az ezred HIRIF a felelős.

A hadműveleti elöljáróval történő nyílt és védett kapcsolattartást minden esetben a KFOR MNTF-W tervezi és szervezi. Az összeköttetést a magyar fél eszközeivel kell végrehajtani abban az esetben, ha az elöljáró nem rendelkezik a zászlóalj számára átadandó híradó eszközök biztosításáról. Amennyiben az elöljáró rendelkezésre bocsát az MH KFOR Z részére híradó-, információvédelmi- és informatikai berendezéseket, azt a magyar félnek át kell vennie, és fel kell készülnie annak használatára.

Az elsődleges összeköttetési lehetőség az elöljáró irányába NATO IVSN rendszeren keresztül valósul meg, amelynek tartaléka az Iridium, Inmarsat műholdas eszközök, és a helyi GSM mobiltelefon készülékek.

2.2. A KFOR Zászlóalj műveleti híradása

A válságkezelő és béketámogató művelet (konvoj-, VIP kísérés, területbiztosítás, objektumvédelem, stb.) eredményes végrehajtása érdekében, a vezetés és irányítás híradó biztosítására hadműveleti híradás került megszervezésre. A hadműveleti hírrendszer tartalmazza a helyi kapcsolatrendszert - a belső összeköttetéseket a táboron belül -, illetve a zászlóalj kapcsolattartási rendjét a különböző műveletek végrehajtása során. A híradó intézkedésben meghatározott összeköttetési formák és a megadott rádióforgalmi rendszerek mellett a híradó és informatikai részleg (S6) önállóan tervez és szervez híradást az adott feladat végrehajtó állománya számára, az elöljáróval együttműködve, figyelembe véve az esetleges együttműködést más alegységekkel, szervezetekkel.

A tábor területén, a belső kapcsolatrendszer kialakítása elsődlegesen a távbeszélő központ mellékeivel kerül kialakításra, amely a vezetékes összeköttetés előnyeinek kihasználását célozza meg. A rendelkezésre álló HIK konténerben telepített központ mellékeit a meghatározottak szerint[17] kell telepíteni. A fel nem használt mellékek tartalékot képeznek az esetleges, előre nem látott igények kielégítésére, az elöljáróval történt egyeztetést követően. A zászlóaljparancsnok, a hadműveleti ügyeletes (HDM Ü) szolgálat, és a telefax berendezés számára rendelkezésre bocsátott mellékek mellett, a magánbeszélgetések biztosítására telepített végberendezésekhez, és a helyi közcélú bérelt fővonalakhoz is mellékek vannak hozzárendelve a központon keresztül. A helyi elhelyezés területén belül a vezetékes összeköttetés mellett kis teljesítményű kézi ultrarövidhullámú

16 Futár és tábori posta híradó eszközöknek nevezzük mindazokat a híradó eszközöket, amelyek az információcsere lehetőségét, a hírváltás megvalósítását írásbeli küldemények továbbításával biztosítják. Az írásbeli küldemények lehetnek szolgálati és magán küldemények. Az FTP eszközökkel szervezett híradást nevezzük FTP híradásnak.

17 Intézkedés a zászlóalj híradó biztosítására

(URH) rádiókészülékeket is fel lehet használni a kapcsolattartás céljából, illetve a helyi GSM eszközöket, a megfelelő szabályozottság mellett, eseti lehetőségként más eszközök kiesése okán.

A KFOR Z a számára meghatározott feladatok végrehajtása során elsődlegesen RH és URH rádiókkal, különböző rádióforgalmi rendszerek felhasználásával teljesítik a kijelölt teendőket. A zászlóalj a kiadott rádióforgalmi rendszereket alkalmazza, de a rádióforgalmi rendszerek összetételét a hadműveleti területen kapott feladatoknak megfelelően az S6 részleg tervezi és szervezi, a hadműveleti- és a honi elöljárójával történő egyeztetésnek megfelelően. A meglévő híradó-technikai eszközök harcászat-technikai adatainak ismerete nélkülözhetetlen a részleg számára, mivel a kompatibilitás, a teljesítmény és egyéb adatok nagyban befolyásolják a felhasználásra kerülő eszközök kiválasztását. Természetesen a feladat típusa és a rendelkezésre álló eszközök is meghatározóak a tervezés során. Fontos, és kiemelt figyelmet kell fordítani a frekvencia felhasználásra és az üzemeltetett rádióforgalmi rendszerek időszerű meghosszabbítására, amelyet a hadműveleti elöljáró kijelölt szervezetével, a frekvenciamenedzsmenttel kell egyeztetni. A hadműveleti területen felkészült szakemberek végzik ezt a munkát, mivel a különböző rádióforgalmi rendszerek együttműködése – zavarás nélkül – elsőszámú kérdése a sikeres műveleteknek. „A hadszíntér átfogó frekvenciamenedzselése viszont minden műveletben előtérbe kerül, és csak kellően felkészült szakemberek képesek egyrészt a frekvencia-koordinációra a civil és katonai rendszerek között, másrészt az eszközök egymás zavarása nélküli üzemének biztosítására.” [11] A frekvenciaigényeket az előírásoknak megfelelő formanyomtatvány felhasználásával kell továbbítani a híradó- és informatikai részlegnek. „Külföldi misszió esetén, a helyszínen felmerült szükségleteket a területileg illetékes frekvenciagazdálkodási szervezethez kell benyújtani a NATO-eljárásban elfogadott frekvenciaigénylés, vagy az illetékes szervezet által meghatározott formanyomtatványon” [12]

A többnemzeti műveletekben résztvevő országok alegységeinek biztosítani kell a saját hadműveleti és az elöljáró irányába történő kapcsolattartás érdekében szervezett és biztosított rádióforgalmi rendszerek frekvencia felhasználásának lehetőségét, amely csak központosított frekvencia kiosztással valósítható meg. Mivel az adott műveleti területen szolgáló nemzetek erői a vezetés és irányítás érdekében rádióforgalmi rendszereket üzemeltetnek, ezért elengedhetetlen az elöljáró által végrehajtott frekvenciamenedzselés, hogy a különböző káros hatások – mint például a rádiók-, illetve az egyéb rádiós frekvencián működő eszközök zavarása – ne okozzanak összeköttetési problémákat a feladatok végrehajtása során. Minden résztvevő számára folyamatos hozzáférhetőséget kell biztosítani az elektromágneses spektrum frekvenciáihoz. A rendkívüli mobilitás, amely a nemzetközi műveleteket jellemezi, megköveteli a hang-, adat kommunikáció érdekében a spektrum széleskörű hozzáférését. Bár missziókban résztvevő nemzeti erőik kommunikációs eszközei, lehetőségei eltérőek, az igényük a frekvenciák felhasználásra azonos, mivel a rádióösszeköttetés alapvető feltétele a sikeres műveleteknek. Ezért is kell nagy figyelmet fordítani a frekvenciagazdálkodásra, amely természeténél fogva összetett, bonyolult tevékenység. A műveletekben részt vállaló koalíciós országoknak ismerniük kell az eljárásmódokat, megállapodásokat és normákat, amelyek szükségesek a kommunikációs és informatikai rendszerek együttműködéséhez.

Amennyiben menethíradást kell szervezni (oszlopkísérés, menetbiztosítás), a hadműveleti elöljáróval minden esetben egyeztetni kell a híradás rendszerét. A menet megszervezése mindenoldalú biztosításának egy kiemelten fontos eleme a menetoszlop híradása. A tervezés és szervezés időszakában különös figyelmet kell fordítani a felhasználásra kerülő híradó eszköz összetételére. A menetoszlop minden gépjárművének rendelkeznie kell híradó berendezéssel, a menethíradásra szervezett rádióforgalmi rendszerbe való belépéssel. A kiképzés és felkészítés során, amelyen a kontingens állománya részt vett a kiutazást megelőzően, elsajátította az alkalmazásra kerülő rádióeszközök felhasználói szintű kezelését. A menet megkezdése előtt meg kell győződni arról, hogy mindenki ismeri mind az elsődleges, mind a tartalék összeköttetési lehetőségeket. Ellenőrizni kell a rádiók

működőképességét és az összeköttetés meglétét. A menethíradás elsődlegesen kisteljesítményű URH rádiók felhasználásával kerül megvalósításra, amely a menetoszlop vezetését biztosítja. A kapcsolattartás a vezetési ponttal (tábor) RH rádióforgalmi rendszerrel kerül megszervezésre.

A menetrend összetételének meghatározása mellett tisztázni kell a felhasználásra kerülő rádiók típusait, amelyek biztosítják az információáramlást az oszlopon belül, illetve a menetoszlop és az alaptábor között. Az oszlopparancsnok a rádióforgalmi rendszeren keresztül ad utasításokat a gépjármű-, harcjármű parancsnokoknak, illetve vesz jelentéseket a biztosítóktól az esetleges vészjelzésekről, és a menetet befolyásoló tényezőkről. A menet híradó támogatása lehetővé teszi, hogy a menetoszlop parancsnok:

- folyamatosan tudja biztosítani a menet irányítását;
- az esetleges beavatkozásokat végre tudja hajtani;
- minden információt megkapjon a járművek helyzetéről és az esetleges meghibásodásokról;
- a forgalmi rendszer tagállomásait folyamatosan értesíteni tudja az esetleges veszélyekről;
- kapcsolatot tartson a táborral az esetleges parancsok, információk vételére;
- végrehajtsa a jelentéseket az elöljáró irányába.

A menetoszlop megindulását megelőzően minden esetben a HDM Ü-nek jelenteni kell az összeköttetés lepróbálását, a híradó eszközök állapotát és a kapcsolatok meglétét. A folyamatos vezetés érdekében minden esetben ki kell jelölni tartalékot, amely az esetleges meghibásodás, megszakadás esetén kerül felhasználásra.

A menetek végrehajtása során MEDEVAC, megerősítő erők igénylésének megszervezését az elöljáró hajtja végre. A MEDEVAC kérést az előírt szabályok betartása mellett kell alkalmazni, amely a mindenkori mentési-, kiürítési feladatokat segíti és gyorsítja. A segélykérő rendszer adatait (forgalmi adatok) legalább járműparancsnoki szintig ismerni kell, amely tartalmazza a frekvenciát, kódokat, az igénylés módját, a jelentéseket.

A KFOR Z kapcsolattartási lehetőségeinek – a műveleti feladat végrehajtásakor – további eleme a helyi SIM kártyás mobiltelefon készülékek, amelyek a katonai rádiók tartalékát képezik. Abban az esetben, ha a tábor irányába kezdeményezett hívásra kerül sor, minden esetben a hírközpont helyi közcélú hívószámát kell hívni.

A hadműveleti feladatok híradó biztosításának tartalékaként hordozható Inmarsat és Iridium egyedi műholdas eszköz kerül kiadásra. Ennek érdekében, a tábor területén, a HDM Ü.-nél folyamatosan biztosítani kell a hívások fogadását, amelyet a készülékek állandó vételkészségben tartásával lehet elérni. A zászlóalj felszerelési jegyzékében lévő híradó eszközöknek rendelkezniük kell a meghatározott okmányokkal, amelyek pontos és részletes vezetése kötelező érvényű az előírt rendszabályok betartása mellet. A missziós feladatok végrehajtásának teljes idejére az előírásoknak megfelelő okmányokkal – forgalmi eseménynaplók, rádióforgalmi rendszer adatlap, vezetési tábla, stb. – való ellátottságának biztosítva kell lennie. A Magyar Honvédségben érvényben lévő Hír/3[18] szakutasítás alapján kerülnek felhasználásra a hívójelek, hívónevek, indexek a rádióforgalmi rendszerek megtervezése során.

A kontingens állománya részére a magánbeszélgetések biztosítása érdekében kihelyezett nyilvános mellékek kerülnek telepítésre, amelyek használatának rendjét a parancsnok szabályozza, amely ismertetésre kerül a személyi állomány előtt. A telefonbeszélgetések „R beszélgetés” rendje szerint történnek.

18 Magyar Honvédség Rádióforgalmi Szakutasítása

A KFOR zászlóalj 2008. szeptember 1-jén kezdte meg tevékenységét, amelyet 2009. szeptember 1-jétől KFOR Kontingens (KFOR KONT.)[19] megnevezéssel folytat tovább napjainkban is. Az új alegység továbbra is zászlóalj szintű ideiglenes katonai szervezet, amely kiválóan teljesíti a vállalt feladatokat.

Az alfejezetet röviden összegezve és értékelve megállapítható, hogy a balkáni békefenntartó műveletekben résztvevő magyar kontingensek ideiglenesen létrehozott, zászlóalj szintű katonai szervezetek, amelyek rendeltetése az adott régió biztonságának és békéjének fenntartása. A magyar alegységek mindkét esetben az MH ÖHP (MH SZFP) szolgálati alárendeltségében, és a KFOR erők valamely magasabb parancsnokság (KFOR parancsnokság; KFOR MNTF-W) parancsnokának műveleti irányítása alatt hajtja végre a számára kijelölt és meghatározott feladatokat.

Magyarország irányába VSAT összeköttetés biztosít hang-, fax- és adatkapcsolatot az MH zártcélú távközlő hálózatába, bérelt szolgáltatás keretén belül, amelyen az Internet és a HM Intranet is biztosított. (MH ŐBZ VSAT csak hangátvitel) Tartalék kapcsolattartásra Inmarsat és Iridium egyedi műholdas berendezések, IVSN kapcsolat, magyarországi SIM kártyás GSM, és RF-5200-as RH rádió került felhasználásra. Az írásos szolgálati- és magánküldemények továbbítását az MH 64. Logisztikai ezred végezte a kontingensek és Magyarország között.

A hadműveleti elöljáró irányában létesített kapcsolatot, és a felhasználásra kerülő eszközöket minden esetben az elöljáró szervezi, biztosítja. Az elsődleges összeköttetés IVSN hálózaton kerül megvalósításra, amely tartaléka egyéb rendelkezésre álló műholdas eszközökkel, esetlegesen GSM készülékekkel kerül megszervezésre. A védett információtovábbítás eszközeit szintén az elöljáró biztosítja az alárendelteknek.

A hadműveleti feladatokat (objektumvédelem, ellenőrzés, konvojkísérés) támogató híradás minden esetben a kijelölt erők és a feladatellátás függvényében kerül megszervezésre. A táboron belüli híradás elsődlegesen vezetékes kapcsolatokkal kerül kiépítésre, illetve szükség esetén kis teljesítményű URH rádiókészülékekkel, helyi SIM kártyás GSM telefonokkal. A konvojok kísérése esetén a menethíradás URH és RH rádiókkal, tartalékként Inmarsat és Iridium műholdas eszközökkel, illetve ezek kiesése esetén GSM telefonokkal kerül végrehajtásra. A hadműveleti területen kiutalt frekvenciák minden esetben az elöljáró frekvenciamenedzsment szolgálata által kerül jóváhagyásra.

3. A MAGYAR HONVÉDSÉG IRAKI SZABADSÁG HADMŰVELET[20] BÉKETÁMOGATÓ MŰVELETEIBEN VALÓ SZEREPVÁLLALÁSÁNAK HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSA

Magyarország az iraki válság rendezése érdekében, az ENSZ BT 1483[21]. számú határozatában elfogadottak szerint kezdte meg politikai előkészítő munkáját.

2003. április 25-én az Amerikai Egyesült Államok levélben kérte fel a Magyar Kormányt az iraki válság rendezésében való részvételre, de ekkor még nem született meg az ENSZ határozata. [13] Az Országgyűlés 2003. május 6-i 54/2003 OGY határozatában fogalmazta meg Irak újjáépítéséhez szükséges stabilizációs feladatokban részt vevő nemzetközi erők tevékenységének nemzeti támogatását. A későbbi egyeztetések eredményeként 2003. november 5-én, a 65/2003-as OGY határozatban döntöttek a magyar katonai hozzájárulásról

19 32/2009. (VI. 5.) HM határozat A Magyar Honvédség Összhaderőnemi Parancsnokság alapító okiratának módosításáról

20 Operation Iraqi Freedom

21 2003. május 22-i 1483. sz. ENSZ BT határozat, a háború utáni iraki „hatóságról", és az ENSZ különleges képviselőjének hatásköréről. „Csütörtökön az ENSZ Biztonsági Tanácsa 14 szavazattal elfogadta az iraki rendezésről szóló hármas javaslatot (Szíria korábban jelezte, hogy a tervezet elfogadhatatlan számára, ezért nem vett részt a szavazáson). A határozat lényegében azt jelenti, hogy a világszervezet utólag legalizálta az addig hatályos nemzetközi jog, az ENSZ BT ellenében indított iraki háborút, elismerve, hogy ami ezután a háborút követő rendezés keretében Irakban történik, az a világszervezet felhatalmazásával történik.[16]

a stabilizációs és humanitárius műveletek elősegítése érdekében. Ennek érdekében egy maximálisan 300 fős, a szükséges technikai eszközökkel, fegyverzettel, felszereléssel ellátott katonai kontingens létrehozását határozta meg, amely feladata szállítmányozási és humanitárius tevékenységek végrehajtása volt Irak területén. A határozatban a kontingens feladatai ellátásának idejét az alábbiak szerint szabályozta: „A Kontingens feladatát 2004. december 31-ig terjedő időszakban, de legfeljebb 6 hónapos időtartamban láthatja el. A külföldi műveleti területen történő tartózkodás idejébe a helyszíni felkészülés, valamint a kitelepülés időtartama nem számít be;". [14] A későbbiekben, 2003. november 5-én az Országgyűlés módosította a felajánlott kontingens feladatellátásának maximális idejét. A határozat szerint 2004. december 31-ig terjedő időszakban hajthatja végre a tevékenységét. [15]

Az iraki koalíciós erők Irak területén négy hadműveleti zónában hajtották végre a feladataikat. Két amerikai hadosztály, egy lengyel vezetésű többnemzeti-, és egy angol vezetésű többnemzeti hadosztály került megalakításra, akik a stabilizációs feladatokat hajtották végre. A létrehozott magyar kontingens, az MH Szállító Zászlóalj (MH SZZ) az úgynevezett Központi- Déli Koordinációs Zónában (KDKZ), a lengyel vezetésű Többnemzeti Hadosztály (MND-CS: Multinational Division Central-South) alárendeltségében végzett főként szállítmányozási feladatokat. Lengyelország 2003 júniusában kezdte meg a KDKZ-ban feladatot teljesítő hadosztályparancsnokság felállításának előkészületeit, majd három hónap múlva átvette az amerikai féltől a térség irányítását.

A hadosztály fő feladata a közigazgatás, a térség stabilitásának helyreállítása és az esetlegesen kialakuló fegyveres küzdelmek, tömegtüntetések megakadályozása, amelyet 29 nemzet mintegy 9000 katonája hajtott végre. Az instabil biztonsági helyzetben folyamatos támadások érték a koalíciós erőket, amelyek tovább nehezítették a munkájukat. A hadosztály a területet önállóan irányította, de a vezetési szintek közötti kommunikáció gyakran akadozott, amely problémát tovább növelte a koalíciós nemzetek közötti együttműködési képesség hiánya.

Az MH SZZ kiküldése a műveleti területre – eleget téve az ENSZ BT felkérésnek – nagyban járult hozzá a térség stabilitása megteremtésének elősegítésében. A zászlóalj első 292 főből álló állománya a kiképzést és felkészítést követően, szállítási (élelem, ruházat, humanitárius segély), logisztikai és egészségügyi feladatokat látott el. Az állomáshelyük Al-Hillah település területén volt, a hadosztály más nemzeteivel közösen. Az MH SZZ feladatainak meghatározása során nemzeti korlátozások lettek kialakítva az alegység biztonsága érdekében, melyek a következők voltak: csak szállítási feladatokat láthatott el az alegység; a zászlóalj nem volt megosztható, részeiben más nemzet parancsnoksága alá nem volt rendelhető; szállítmánykísérés csak a saját, magyar parancsnokság alá tartozó menetoszlopok részére volt engedélyezett.

A kontingens híradó- és informatikai rendszerének biztosítania kellett az összeköttetést az elöljárók irányába (hadműveleti, nemzeti), a táboron belül, és a feladatok végrehajtása során az alegységek között.

A zászlóalj híradó- és informatikai rendszere a számára rendszeresített katonai, valamint a polgári távközlési és informatikai eszközök – VSAT, GSM, stb. – és szolgáltatások felhasználásával került biztosításra. A zászlóalj elsődleges feladatából – szállítás – adódóan kiemelt hangsúlyt kellett fektetni a menetoszlopok híradó támogatására, amely a feladat végrehajtásának vezetés és irányítási feltételeit biztosította. A következőkben a zászlóalj híradó rendszerével, az elöljáró irányába történő kapcsolattartással, és a hadműveleti híradás vizsgálatával foglalkozunk, amely meghatározza a kialakított híradó- és informatikai rendszert.

3.1. A Szállító Zászlóalj híradása az elöljárókkal

A zászlóalj elöljáró irányába szervezett híradása a lengyel hadosztállyal és a hazai parancsnoksággal létesített összeköttetéseket tartalmazza. Az iraki magyar kontingens nemzeti elöljáró parancsnoksága az MH ÖHP jogelődje, az MH SZFP[22] volt. A kontingens tevékenységéről és egyéb logisztikai biztosításról – javítás, utánpótlás, stb. – történő folyamatos jelentés és tájékoztatás érdekében híradást kell szervezni a nemzeti elöljárók irányába. Az elsődleges összeköttetési út bérelt VSAT műholdas szolgáltatással került biztosításra Magyarország irányába. A Magyar Honvédség iraki missziója alkalmával alkalmazott elsőként szélessávú, integrált szolgáltatású VSAT rendszert, amely az MH ŐBZ által használt hangalapú kommunikációt váltotta fel.

A VSAT összeköttetés biztosította a hang- és az MH Intranet és Internet szolgáltatásokat a zászlóalj számára Magyarország irányába. Az Intranet szolgáltatás felhasználásával valósult meg a hazai parancsnokságok irányába történő elektronikus levelezés, a levelező- illetve az általános célú információs szolgáltatás a Portál rendszer[23]. Az informatikai szakállomány feladata az informatikai hálózat kiépítése, üzemeltetése volt, és ennek érdekében az együttműködés a Magyar Honvédség Híradó Parancsnokság Ideiglenes Országos Informatikai Hálózat-felügyelet (MH HIP IOIHF) szakembereivel. A rendszer két alapvető egysége a Geostacionárius Föld körüli pályán mozgó műholdon (GEO: Geostationary Earth Orbit) lévő átjátszók, és a földi telepítésű terminálok. Nagy előnye, hogy nincs szükség fizikai vonal kiépítésére, csupán a végberendezéseket kell telepíteni, üzembe helyezni. A kiképzett állomány legfeljebb 4 óra alatt telepítheti a VSAT terminált. A nagy távolságot biztosító szolgáltatás így gyorsan elérhető. További előnye a kis méret, a flexibilis kiépítés, és nagysebességű folyamatos átvitelt biztosít, amely megbízható összeköttetéssel párosul. Missziós alkalmazásra kiváló, mivel a földi infrastruktúrától független, bárhol telepíthető, és miután zárt rendszert alkot, így nagy kommunikációs adatbiztonságot nyújt, amely elengedhetetlen követelmény a katonai alkalmazás területén. A missziós alkalmazást jelentősen nem befolyásolja a VSAT összeköttetés esetén fellépő késleltetés[24], ezért, és a távolság-független átviteli költség okán kiválóan felhasználható a nemzetközi katonai műveletekben, mint az iraki válság rendezésében. Ezen kommunikációs összeköttetés tartalékaként kerültek felhasználásra az Inmarsat és Iridium műholdas telefonkészülékek. Az Iridium készülékeket elsőként az MH SZZ alkalmazta, amely megbízható összeköttetést biztosított az alegység számára a műveletek végrehajtása során. A két készülék honi híradás biztosítására, szolgálati beszélgetés kezdeményezésére a rendkívül magas költségek miatt csak kivételes esetben volt alkalmazható, ezért minden alkalommal szükséges volt a parancsnok engedélye, és a híradó tiszt felelőssége.

A hazai kapcsolattartás érdekében egy RH rádióforgalmi rendszer került megszervezésre, amely a zászlóalj és a magyar elöljáró között biztosított összeköttetést. A hírközpont konténerben telepített RF-5200-as rádió a harmadlagos honi kommunikációt volt hivatott ellátni, amelyet csak erre a célra lehetett felhasználni. Más feladatok híradó támogatására

22 „A Magyar Honvédség Szárazföldi Parancsnokság, a Magyar Honvédség Légierő Parancsnokság megszüntetésével, azok jogutódjaként, illetve a megszűnő Magyar Honvédség Összhaderőnemi Logisztikai és Támogató Parancsnokság, a Magyar Honvédség Híradó és Informatikai Parancsnokság, a Magyar Honvédség Művelet Irányító Központ és a Magyar Honvédség Egészségügyi Parancsnokság egyes feladatainak át vételével, 2007. január 1-jei hatállyal megalakult az MH Összhaderőnemi Parancsnokság.” [17]

23 A portál olyan alkalmazás, amely lehetővé teszi, hogy a szervezet/szervezetek a meglévő vagy külső információikat közöljék, ezen információkhoz a felhasználók számára egy felületen, személyre szabottan hozzáférést biztosítsanak, illetve egyesítik, kezelik, elemzik és terjesztik az információt a szervezeten belül. Az MH portálrendszeren a személyi állomány különféle információkat, szolgáltatásokat (szolgálatvezénylés, meteorológia) érhet el.

24 Az egyes alkalmazások használatakor, illetve tervezésekor figyelembe kell venni, hogy a műholdas adatátvitel a földfelszíni távközléshez képesti viszonylag magas jelterjedési késleltetéssel bír a jelentős műhold – Föld távolság miatt.

csak átmeneti jelleggel, szükséghelyzetben, minden más összeköttetési forma kiesése esetén, a parancsnok engedélyével lehetett alkalmazni. A rádiót a rejtjelző moduljával kiegészítve kellett alkalmazni a szolgálati közlemények továbbítására, a megfelelő biztonság elérése érdekében. A rádiókészülék minden esetben ügyeletes vétel üzemmódban kellett, hogy legyen. A megbízható kapcsolat biztosítása érdekében, heti összeköttetés felvétel lett elrendelve, amely során minőség-ellenőrzést kellett végrehajtani. A telepítést követően jelentős problémát jelentett, hogy a készülék zavarta a tábori könnyűvezetékkel (TKV-100) kiépített belső kommunikációs hálózatot (a fellépő indukciós feszültség következtében). A probléma a hazai gyakorlások alatt nem jelentkezett, mivel a készülék telepített antennája távolabb volt elhelyezve, amit a magyar tábor elhelyezése esetén – szűkös települési körzet – nem lehet megvalósítani. [18] Az optikai vezetékek felhasználása, illetve az antenna sugárzásának figyelembe vételével történő telepítés megoldotta ezt a problémát, de mivel csak tartalék összeköttetés ez az rfr., így nem okozott komolyabb fennakadást a zászlóalj számára.

Az MH Szállító Zászlóalj nyílt, szolgálati illetve magánküldeményeinek továbbításának - az FTP híradás megvalósításának – felelőse az MH 64. Boconádi Szabó József Logisztikai és Támogató Ezred híradó főnöke volt. A küldeményeket a HM és az MH Titokvédelmi és Ügyviteli Szabályzatában[25] meghatározottak szerint lehetett továbbítani.

A lengyel vezetésű Többnemzeti Hadosztállyal (műveleti elöljáró) történő kapcsolattartást a hdo. nyílt- és védett híradó és informatikai rendszeréhez történő kapcsolódással került megvalósításra, az együttműködés és a vezetés feltételeinek megteremtése biztosítása érdekében. A kapcsolat megtervezéséért, megszervezéséért és biztosításáért az elöljáró volt a felelős. A kontingens feladata a szolgáltatásokhoz történő hozzáférés érdekében az alkalmazások biztosítása és a felhasználók felkészítése volt. A parancsnok feladata volt továbbá a műveleti elöljárótól érkező irányalegység fogadásának előkészítése. Az elsődleges összeköttetést - amelyet az elöljáró biztosított -, TCE-500/B[26] rejtjelző készülékkel került megvalósításra, amely hang-, adat-, és fax kapcsolatot tett lehetővé. A készülék üzemeltetését a kiadott üzemeltetési szabályzat és kezelési utasításoknak[27] megfelelően kellett végrehajtani. Az eszköz telepítéséhez, üzemeltetéséhez, felügyeletéhez felkészített szakembereket kellett alkalmazni. Az S6 vezetője a rejtjelzési felelős[28], a híradó tiszt pedig a rejtjelfelügyelő[29] feladatokat látta el. A parancsnok rendelkezett az át nem ruházható titokvédelmi felügyelő[30] jogkörrel. Kiemelten fontos ezen eszközök telepítési helyének meghatározás, amely csak és kizárólag folyamatosan felügyelt, őrzött helyiségekben volt lehetséges, amely biztosította az illetéktelen személyek távoltartását a készüléktől.

Az Többnemzeti Hadosztály irányából továbbá egy parancsnoki rádióforgalmi rendszer került kialakításra a vezetés biztosítása érdekében, illetve a logisztikai támogatásra egy logisztikai rfr. Az összeköttetés technikai feltételeit, a forgalmi rendszer összetételét, és a zászlóalj forgalmi adatokkal való ellátását az elöljáró biztosította.

25 Ált/3 A Honvédelmi Minisztérium és a Magyar Honvédség Titokvédelmi és ügyviteli szabályzata. (HM kiadás 1996)

26 TCE-500/B.: Keskenysávú titkosító berendezés, amely titkosított hang- és adat kommunikációt biztosít végpontok között bármely típusú telekommunikációs hálózatban.

27 A 48/6-R Honvédelmi Minisztérium Honvéd Vezérkar Vezetési Csoportfőnökség, 48/13-R Honvédelmi Minisztérium Honvéd Vezérkar Hiradó és Informatikai Csoportfőnökség számok alatt kiadott szabályzatok.

28 Az a személy, aki a rejtjelző eszköz rendelkezésre állásának biztosítására, a konfigurációs módosítások végrehajtására, a vonatkozó rendszabályok betartatására és a felhasználók felkészítésére, ellenőrzésére kijelölt személy.

29 A rejtjelfelügyelő feladata az elöljáró rejtjelfelügyeletekkel való kapcsolattartás, az eszközökkel kapcsolatos biztonsági követelmények érvényesítése, a vészhelyzeti terv elkészítésére és folyamatos frissítésére, és a szabályok ellenőrzése felhatalmazott személy.

30 „titokvédelmi felügyelő: az a személy, aki a titokbirtokos szerv vezetőjének felhatalmazása alapján irányítja és ellenőrzi a titokvédelmi feladatok végrehajtását” [19]

3.2. A Szállító Zászlóalj hadműveleti híradása

A zászlóalj belső kapcsolatrendszerének kialakítása az Ideiglenes Állományjegyzék és az Ideiglenes Felszerelési jegyzékben[31] szereplő híradó- és informatikai eszközök felhasználásával került kialakításra, az alegység vezetés és irányításának céljából. Az alegység hadműveleti híradása három fő területre volt bontható, amely biztosította a széleskörű információváltást a meghatározott szervezetek között.

A zászlóalj belső összeköttetése távbeszélő-, kisteljesítményű URH- és informatikai eszközök felhasználásával került biztosításra. Jelen esetben a helyi sajátosságok és a távközlési infrastruktúra állapota miatt, nem lehetett összeköttetést tervezni a meglévő nemzeti (helyi) kommunikációs hálózatra. A magyar tábor elhelyezési körlete vezetékes híradásának kialakítása a HIK konténerbe telepített HICOM-330 távbeszélő központ felhasználásával került megvalósításra. A vezető szervek, végrehajtó- és kiszolgáló munkahelyek, szolgálatok és pihenők vezetékes híradása alkotta a kontingens belső híradását. A központ programozását műholdas kapcsolattal az MH HIP Országos Hálózatfelügyeleti Főközpont (OHFK)[32] kapcsolástechnikai felügyelője végezte, a fizikai kiépítést pedig a rendszeresített szakállomány. A szervezés, tervezés és a kialakítás során figyelembe kellett venni a prioritásokat, mely szerint a parancsnok, a szállítmányozási feladatok irányításáért felelős mozgáskoordinációs központ és a hadműveleti részleg részére elsődlegesen kellett biztosítani áramköröket, kizárólagos hozzáféréssel, állandó rendelkezésre állással.

A belső híradást a rendszeresített erők, eszközök felhasználásával a híradó részleg szervezi tervezi. A VSAT berendezés, az Inmarsat műholdas telefonok, a telefax eszközök, a TCE-500 titkosító eszköz, az Automata Mérő és Adatgyűjtő Rendszer (AMAR)[33] (egység) illetve a munkahelyek, pihenők irányába ki kellett rendezni a megfelelő számú mellékeket, amelyek biztosították a megfelelő információáramlást. A kialakított mellékek mellett tartalékot is kellett képezni, az előre nem látható igények kielégítése céljából. Természetesen a kialakítást követően elkészítésre kerültek a telefonjegyzékek, amelyek a belső kapcsolattartás fontos elemei. A bagdadi nagykövetségre kikülönített speciális feladatokat ellátó részleggel együttműködési híradás került megszervezésre Iridium eszköz felhasználásával.

A zászlóalj alaprendeltetéséből adódóan kiemelt hangsúlyt kell fektetni a menetoszlopok összeköttetésének, a menethíradásnak biztosítására. A mozgáskoordinációs központ részére két RH és egy URH rádióforgalmi rendszer, Iridium műholdas telefon és Inmarsat eszköz volt biztosítva. (Az Inmarsat eszköz Fax berendezés végződtetéssel is el volt látva a küldemények adás-vételére.)

Az elsődleges rfr. az RF-5200-as rádióval lett szervezve, amely kiesése esetén a másik két rfr. volt felhasználható. A vezető állomás minden esetben a központ volt a feladat végrehajtás során, de a menetoszlop parancsnoka tartalékként, és az előírt bejelentkezési

31 A nemzetközi műveletekben résztvevő alegységeket nem egy meglévő MH szervezetből különítik ki, hanem egy ideiglenes katonai szervezetet kerül megalakításra. A létrehozott szervezet – jelen esetben az MH SZZ – ideiglenes állományjegyzékkel és felszerelési jegyzékkel rendelkezik, amely az adott katonai szervezetre vonatkozik, és biztosítja mind a személyi, mind a technikai feltételeit a küldetésnek. Mindezek a meghatározott tevékenység végrehajtásának befejezéséig kerülnek kiadásra.

32 Az MH HIP 2001 és 2005 között működő katonai szervezet, amely 2005-től 2007-ig az MH Híradó és Informatikai Parancsnokság nevet vette fel, majd a haderő átalakítás során megszűnt, és 2007-től az MH Támogató Dandár, mint új szervezet került megalakításra az állomány egy részének ”beolvasztásával”.

33 „Az AMAR rendszer összetevőit az AMAR központ és a mérőállomások alkotják. A mérőállomások meteorológiai és sugárzásmérő érzékelőinek adatait az állomás számítógépe gyűjti és jeleníti meg táblázatos formában. A mérőállomások adatait a központi számítógép rendszeres időközönként kérdezi le és ennek elemzése alapján alakítja ki a sugárhelyzetre vonatkozó értékelt információkat, illetve szükség esetén hajtja végre a riasztást. … Az AMAR rendszer mérőállomásainak informatikai összetevői szünetmentes tápegységgel, speciális illesztő kártyával és telefonos modemmel ellátott személyi számítógépek. A mérőállomás lehet telepített, illetve gépjárműbe, vagy akár helikopterbe épített változat.” [20]

feladatokon kívül átvehette a vezetőállomás szerepét a tagállomások irányába. A menetoszlopok részére minden esetben összeköttetést kellett szervezni a mozgáskoordináló központtal. Az RF-5200-as rádiókkal szervezett rádióforgalmi rendszerek a rejtjelző modul felhasználásával kerültek alkalmazásra a szolgálati közlések továbbítása érdekében.

A konvojok (menetoszlopok) részére két darab URH és egy RH rádió volt biztosítva. Az oszlop elsődleges vezetése URH rádióval történt, a parancsnok 1. számú URH rádióforgalmi rendszerével. A vezető állomás a forgalmi rendszerben mindenkor a konvojparancsnok. Híváskezdeményezést a tagállomások csak rendkívüli esetben, azonnali közlemény esetén hajthattak végre, minden más esetben ügyeletes vétel üzemmód volt elrendelve. A megtervezett megszervezett, és előzetesen kiadásra került rádióhíradás a feladatok végrehajtásának híradó biztosítása érdekében és az elöljáró intézkedésének megfelelően átszervezhetőek, de az alapelvek mindenkor iránymutatók. A menetoszlop megindulását megelőzően kötelező jelleggel összeköttetés felvételt, csatorna- és frekvenciaváltást, összeköttetés újbóli felvételét kellett végrehajtani. A csatornaváltás ellenőrzése a kijelölt tartalék csatorna felhasználása miatt volt szükség, mivel az összeköttetés megszakadása esetén ez került felhasználásra. A menetoszlop biztosítása érdekében BTR-80/A típusú páncélozott harcjárművek kerültek kijelölésre, amelyek a szállítmánykísérő – biztosító szakaszhoz tartoztak. A parancsnoka részére tűzvezető rádióforgalmi rendszer került megszervezésre, a harcjárműről való szállás esetére.

A katonai rádiókészülékek számára rendszeresített forgalmi eseménynaplók pontos és részletes vezetése alapvető előírás, mely betartását a mindenkori híradó tiszt ellenőrzi. A forgalmi eseménynaplók vezetése a későbbi, esetleges ellenőrzés érdekében kötelező. A hívónevek-, hívószámok kiutalását, a vezetési tábla felhasználását, a szolgálati közlések táblázatának alkalmazását az alapvető előírásoknak megfelelően kellet végrehajtani, amelyért a mindenkori híradó tiszt felelt. A rádióforgalmi rendszerek frekvenciái előzetesen kerültek engedélyeztetésre, de a műveletek során fellépő egyéb frekvenciaigényeket a műveleti elöljáró frekvenciamenedzsmentje irányába kellett felterjeszteni az előírt nyomtatvány felhasználásával. A menetoszlop részére egy rádiókészülék a MEDEVAC kérésre került biztosításra, amely az esetleges egészségügyi mentést biztosította.

A menetoszlopok híradó biztosítása érdekében minden gépjármű és harcjármű rendelkezett URH rádiókészülékkel. A konvojok minden esetben biztosítva voltak 3db BTR-80/A típusú harcjárművel, R-142/M típusú rádióállomással, egy egészségügyi feladatokat ellátó gépjárművel és technikai záró részleggel (TZR). A szállítmányok szállítását tehergépjárművek biztosították a feladat végrehajtása során.

Az MH SZZ alkalmazott elsőként műholdas járműkövető rendszert. A mozgáskoordináló központban és az R-142/M rádióállomáson telepített Inmarsat berendezések elsődleges felhasználása a járműkövető rendszer biztosítása volt, amely lehetővé tette a parancsnok részére a konvojok menetének nyomon követését.

A zászlóalj állománya részére a magánbeszélgetések biztosítása érdekében kihelyezett nyilvános mellékeket telepítettek, amelyek „hotline” üzemmódban voltak szervezve a HM-II (Honvédelmi Minisztérium kettes objektuma) központkezelővel. A használatának rendjét a parancsnok szabályozta, amely ismertetésre került a teljes személyi állomány részére. A telefonbeszélgetések „R beszélgetés” rendje szerint történt.

A zászlóalj a rendeltetésének végrehajtása során jól alkalmazható, összetett kommunikációs rendszer került megszervezésre, megtervezésre. A híradó és informatikai eszközök biztosították a vezetés minden irányú híradó támogatását, amely a sikeres vezetés és irányítás alapvető elemei. Az MH Szállító Zászlóalj a 119/2003. (XI. 5.) OGY Határozatban foglaltaknak megfelelően – a mandátum lejártát követően – befejezte a feladatait Irak területén, és az utolsó váltás hazatelepült, annak ellenére, hogy az ideiglenes iraki kormány felkérte az országot a kontingens mandátumának meghosszabbítására. „Az Magyar Honvédség Szállítózászlóalja, – 2003 júliusától, 2004 decemberéig – a 642 szállítási

feladat során mintegy 2,5 millió kilométert tett meg, 50 ezer tonnányi árut (humanitárius segély, élelmezési, ruházati, erődítési anyagok) szállítva." [21]

4. A MAGYAR HONVÉDSÉG AFGANISZTÁNI BÉKETÁMOGATÓ MŰVELETEIBEN VALÓ SZEREPVÁLLALÁSÁNAK HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSA

A világot megrázó, az Amerikai Egyesült Államokat ért terrortámadásokat[34] követően a nemzetközi terrorizmus vált az egyik legnagyobb veszélyforrássá és egyben kihívássá a világ számára. A támadásokra reagálva az amerikai erők megdöntötték Afganisztánban a tálib rezsimet a Tartós Szabadság Művelet (OEF: Operation Enduring Freedom[35] elnevezésű hadműveletben.

Az ENSZ megkezdte előkészítő tevékenységét – a nemzetközi közösség összehívására –, majd Petersbergben[36] konferenciát tartottak 2001. november 27-e és december 5-e között. [22] Az afganisztáni helyzetről, politikai jövőjéről szóló konferencia utolsó napján a résztvevők aláírták a „bonni egyezményt", amely alapján a biztonságos újjáépítés elősegítésére megalakult a Nemzetközi Biztonsági Közreműködő Erő (ISAF: International Security Assistance Force). Az ENSZ BT 1386/2001-es határozata jóváhagyta az ISAF erők mandátumát, amely engedélyezi a szükséges katonai erők alkalmazását a mandátum teljesítéséhez, továbbá biztosítja az afgán kormány segítségnyújtását.[37]

Magyarország részvételére a kialakult nemzetközi helyzet rendezésében az Országgyűlés 62/2001. (IX.25) és a 65/2001. (X.5.) határozatai alapján került sor első ízben, amelyek kimondják az ország terrorizmus elleni harc támogatását és az ország hozzájárulását adja, hogy az OEF műveletben részt vevő fegyveres erők a művelet időtartama alatt átrepüljenek Magyarország légterén. Az Országgyűlés a 62/2001-es határozatának ötödik pontja szerint, az ország a kollektív védelemben megfogalmazottak szerint jár el. A Magyar Köztársaság Kormánya a 2029/2002 (II.6.)[38] és a 2064/2002 (III.21.)[39] határozataiban engedélyezte az OEF műveletben résztvevő kontingensek és az ISAF erők átvonulását az ország területén.

A magyar részvétel az afganisztáni rendezésben az Országgyűlés 111/2002 (XII.18.)[40] határozata alapján kezdődött meg, felhatalmazást adva egy 50 fős egészségügyi kontingens részvételére 2003. december 31-ig. Később törzstisztek és tiszthelyettesek különböző egyedi beosztásokat láttak el Kabulban és Kunduzban egyaránt.[41] A magyar haderő alegységeinek nagyobb és jelentősebb szerepvállalása 2004-ben következett be, amikor felállításra került az MH Könnyű Gyalog Század (MH KGYSZD)[42]. Az alegység Kabul közelében, norvég zászlóalj-parancsnokság alárendeltségében hajtotta végre járőrözési, objektumbiztosítási, kísérési, biztosítási, és őrzés-védelmi feladatait. Az MH KGYSZD 2006. augusztusig tartó mandátumának lejártával, az ISAF feladatok átadását követően részben kivonásra, részben

34 2001 szeptember 11-én összehangolt terrorcselekményeket hajtottak végre négy eltérített utasszállító repülőgéppel az Amerikai Egyesült Államok ellen. Felelősként az Al-Kaida terrorszervezetet nevezték meg, amelyet az afgán kormány támogatott.

35 Tartós Szabadság Művelet, ami harci jellegű, nem háborús katonai művelet (korábban: Infinite Justice- Végtelen Igazság)

36 Németország középső részén található település.

37 Az ISAF 2002 februárjában kezdte meg működését, és a NATO 2003 augusztusától vette át a vezetését.

38 A Magyar Köztársaság Kormányának 2029/2002. (II.6.) Korm. Sz. határozata a NATO tagállamaihoz tartozó fegyveres erőknek az afganisztáni Enduring Freedom műveletben részt vevő kontingensei Magyarországon történő átvonulásainak engedélyezéséről

39 A Magyar Köztársaság Kormányának 2064/2002. (III.21.) Korm. Sz. határozata az afganisztáni rendezést elősegítő nemzetközi biztonsági közreműködő erők (ISAF) Magyarországon történő átvonulásainak engedélyezéséről

40 Az Országgyűlés 111/2002. (XII. 18.) OGY. Sz. határozata az afganisztáni nemzetközi Biztonsági Közreműködő Erők (ISAF) műveleteiben magyar katonai egészségügyi kontingens részvételéről

41 Az Országgyűlés 99/2003. (X. 10.) OGY Sz. határozata az afganisztáni Nemzetközi Biztonsági Közreműködő Erők (ISAF) műveleteiben való magyar katonai részvételről

42 A 2192/2004. (VII. 21.) Kormány Határozat egy maximum 150 fős alegység kitelepítéséről

átcsoportosításra került az újonnan megalakuló magyar vezetésű Tartományi Újjáépítési Csoportba.

A magyar Tartományi Újjáépítési Csoport 2006. augusztus 1-jén alakult. A szervezeti egység önálló állománytáblával és felszerelési jegyzékkel létrehozott ezred jogállású katonai szervezet. A 2115/2006 (VI. 29.) Kormány Határozat rendelkezik a magyar újjáépítési csoport létrehozásáról. Magyarország 2006. október 1-jétől átvette a Baghlan tartomány PRT vezetését[43], amely a meghatározó feladatokat ellátó nemzetek közé „emelte" a magyar csoportot.

A Honvédelmi Miniszter 78/2006. (HK 16) HM utasításának megfelelően az MH PRT jogállását a következő szerint határozta meg: „magyar Honvédség Tartomány Újjáépítési Csoport, külföldi feladat-végrehajtásra tervezett, miniszteri határozattal létrehozásra kerülő ideiglenes katonai szervezet, amely ideiglenes állománytáblával, ideiglenes felszerelési jegyzékkel, ideiglenes szervezeti és működési szabályzattal rendelkezik, a HM HVK MFCSF nemzeti vezetése és az MH Szárazföldi Parancsnokság szolgálati alárendeltségében áll." [23].

Az MH PRT rendeltetése a tartomány infrastrukturális fejlesztésének és a helyi kormányzati szervek megerősítésének biztosítása; a régió újjáépítési feladatainak elősegítése; a magyar nemzeti feladatok, programok támogatása és irányítása; kapcsolattartás a helyi hatóságokkal, vezetőkkel, a lakossággal és egyéb nemzetközi szervezetekkel.[44] A PRT feladatai a rendeltetéséből adódóan a tartomány biztonságának növelése mellett az oktatási- és közlekedési infrastruktúra és az egészségügy fejlesztése, valamint a helyi lakosság támogatása, a nemzetközi erők jelenlétének elfogadtatása. Összességében megállapítható, hogy a PRT rendeltetéséből és feladatából adódóan hozzájárul a tartomány stabilitásához, fejlesztéséhez és biztonságához. A kontingens kettős vezetése – nemzeti és ISAF –, és a civil és katonai feladatrendszer összetett működésű alegységet eredményezett, amely az alábbi tevékenységeket hajtja végre a kijelölt térségben:

- A tartomány fejlesztésének, újjáépítésének segítése projektek végrehajtásával;
- Táborüzemeltetés, fenntartás, őrzés-védelem;
- Civil szakértők, tanácsadók elhelyezése, ellátása, védelme;
- Civil környezet, helyi lakosság bizalmának elősegítése;
- Általános és katonai információgyűjtés,
- Személyek szállítmányok kísérése, biztosítása;
- ISAF és magyar katonai jelenlét demonstrálása;
- Az MH PRT tevékenységének akadályoztatása esetén, ha szükséges rendfenntartás;
- Segítségnyújtás átvonuló szövetséges erőknek, személyeknek;
- Afgán Nemzeti Hadsereg kiképzésének, felkészítésének segítése;
- Afgán Rendőrség tanácsadással, szakmai képzéssel történő segítése. [24].

A Biztonsági Tanács valamennyi vonatkozó határozataival összhangban az ISAF legfőbb feladata az afgán kormány támogatása a biztonságos és stabil környezet kialakításában. Ennek megvalósítása és elősegítése érdekében öt regionális parancsnokságot hoztak létre, amelyek a felelősségi területükön belül működő PRT-ket irányítják. Az öt parancsnokság különböző vezető nemzetek irányításával működik, amelyek az alábbiak[45]:

- Fővárosi Regionális Parancsnokság (RC /C/: Regional Command Capital)[46];

43 A baghlani tartományi újjáépítési csoportot 2004 – 2006 között Hollandia vezette, üzemeltette.

44 A kontingens több szervezettel együttműködve hajtja végre feladatait, mint az Egyesült Államok Nemzetközi Fejlesztési Hivatala (USAID: United States Agency for International Development); az ISAF által delegált média csoport (ISAF Forward Media Team).

45 A jelenlegi parancsnokságok és a vezető nemzetek (2010. február 01.)

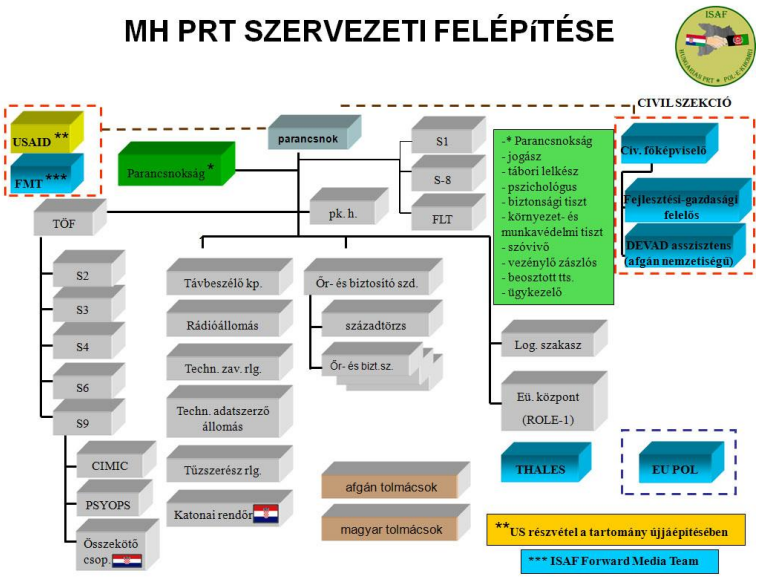
46 Vezető nemzet: Törökország /Franciaország, Olaszország, Törökország folyamatos rotációval/; Az ISAF főparancsnokság, az RC (C) parancsnokság települési helye: Kabul

- Északi Regionális Parancsnokság (RC /N/: Regional Command North) [47];
- Déli Regionális Parancsnokság (RC /S/: Regional Command South) [48];
- Keleti Regionális Parancsnokság (RC /E/: Regional Command East)[49];
- Nyugati Regionális Parancsnokság (RC /W/: Regional Command West)[50].

4. ábra: Az ISAF regionális parancsnokságai és tartományok elhelyezkedése a vezető nemzetek jelölésével Forrás: [25]

A Baghlan tartományban, Pul-i Khumri körzetben[51], a Camp Pannonia táborban állomásozó MH PRT feladatai az előzőekben leírtak alapján igen összetett. Az elsődlegesen a lakosság életkörülményeinek javítását szolgáló civil-katonai együttműködési (CIMIC: Civil-Military Co-operation) projektek mellett a hagyományos értelemben vett katonai feladatokat ellátó kontingens vezetés és irányítását biztosító híradó- és informatikai rendszer kialakítása is jelentős szervezési és tervezési feladatokat követel meg mind az előkészítő, mind a feladatokat végrehajtó csoportoktól. A katonai feladatok úgy, mint az őrzés-védelem, járőrtevékenység, konvoj- és VIP kísérés már az afganisztáni missziót megelőzően is jelen volt a kontingensek feladatrendszerében. Az eltérés az eddigi műveletekhez képest az, hogy egy teljes tartomány biztosításának ellátása a tevékenység alapja, amelyet a hazai (nemzeti) és az ISAF RC (N) parancsnokságok vezetése mellett, más PRT-kal, helyi- és nemzetközi szervezetekkel együttműködve hajtja végre. A híradás biztosításának kialakítását (együttműködési, elöljáró irányába, műveleti) az előbbiekben felsoroltaknak megfelelően kell szervezni és tervezni.

47 Vezető nemzet: Németország; Parancsnokság települési helye: Mazar-e-Sharif
48 Vezető nemzet: Egyesült Királyság /Kanada, Hollandia, Egyesült Királyság folyamatos rotációval/, Parancsnokság települési helye: Kandahar
49 Vezető nemzet: Amerikai Egyesült Államok; Parancsnokság települési helye: Bagram
50 Vezető nemzet: Olaszország; Parancsnokság települési helye: Herat
51 Baghlan tartomány 12 körzetre van felosztva.



5. ábra: A magyar Tartományi Újjáépítési Csoport szervezeti felépítése
Forrás: [26]

A PRT szervezete úgy került kialakításra, hogy a kellő létszámmal és technikai eszközzel felszerelt kontingens végre tudja hajtani a térség stabilizációjának, humanitárius segítségnyújtásának, illetve az újjáépítési munka feltételeinek, biztonságának folyamatos fenntartását, megteremtését és koordinálását.

A szervezeten belül az S6 felel a híradó- és informatikai rendszer szervezéséért, tervezéséért és folyamatos működtetéséért, melynek alaprendeltetése, hogy biztosítsa a kontingens parancsnokának vezetés és irányítási tevékenységét, valamint az elöljárókkal és együttműködőkkel történő kapcsolattartást.

4.1. A magyar Tartományi Újjáépítési Csoport híradása az elöljárókkal

A nemzeti elöljáró parancsnoksággal (MH ÖHP) és más szervezetekkel folyamatos kapcsolattartást kell biztosítani a PRT tevékenységének jelentéséhez, az esetleges javítási, utánpótlási és egyéb információk továbbítása érdekében. Az elsődleges átviteli út Magyarország irányába a VSAT műholdas rendszeren keresztül, bérelt szolgáltatás keretén belül valósul meg. A műholdas átviteli út biztosítja az MH távhívó rendszeréhez, az MH Intranet belső informatikai-, és az Internet hálózathoz való kapcsolódást. Az eszköz telepítését a híradó szakállomány végzi a HIK konténer telepítését követően. Az előírásoknak megfelelően kell elhelyezni a VSAT antennát, hogy biztosítsa a megbízható összeköttetést, illetve a fizikai védelmet egyaránt.

A HIK konténer HICOM-330 központjában végződtetett vonal további kirendezését a központ állománya végzi, a magyarországi oldalon az MH távhívó hálózatába történő integrálását pedig az MH TD biztosítja. A szükséges programozásokat és a híradó- és informatikai hálózat felügyeletét az MH TD OHFK és az MH TD Informatikai Főközpont (IFK) szakemberei végzik. A központ programozása a műholdas terminál modemes kapcsolatával történik.

A kontingens informatikai rendszere biztosítja a már említett Internet hozzáférést, az MH Intranet hálózaton elérhető MH Portál rendszert, levelezőrendszert, a videokonferencia

(VTC: Video TeleConference)[52] kapcsolatot, valamint az irodaautomatizálási rendszert (NIAR: NATO Irodaautomatizálási Rendszer).[53]

Másodlagosan NATO IVSN hálózaton keresztül történő összeköttetés valósítható meg az „anyaországgal". Mivel az IVSN nyílt kapcsolatot biztosít, ezért a minősített információk biztonságos továbbításának elérése érdekében NATO minősített beszéd- és adattitkosítókat kell alkalmazni. Mára az IVSN már nem tartozik a korszerű technológiai megoldások közé, de a rendszer egyes elemei kiszolgálják a felhasználókat, így a NATO és egyes tagállamok még mindig alkalmazzák. Az IVSN hálózat STU II[54] típusú végtitkosító berendezéssel (vagy egyéb titkosító végberendezéssel) kerülhet kiépítésre a minősített távbeszélő kapcsolat megvalósítása érdekében, illetve a telepített minősített munkaállomás felhasználásával érhető el a megfelelő szintű biztonságot nyújtó információtovábbítás.[55] Természetesen az írásos formában elkészült, és továbbításra kerülő fax küldeményekhez biztosítani kell telefax kapcsolatot. Ezek elsődlegesen az MH távhívó rendszerén kerülnek továbbításra, de kerülő irányon a NATO IVSN hálózatán keresztül is biztosítható. Tartalékként a HIK konténerben elhelyezett Inmarsat műholdas eszközre telepíthető telefax berendezés is felhasználható.

A további kapcsolattartási lehetőség, a már „jól bevált", a korábbi missziók során is alkalmazott Iridium és Inmarsat műholdas eszközök felhasználásával valósítható meg, de ezek a készülékek elsődlegesen a hadműveleti híradást biztosítják. Minden műholdas eszköz használata esetén az előírt okmányok – mint például a forgalmi eseménynapló – pontos vezetésére kiemelt figyelmet kell fordítani. A készülékeket csak a meghatározott előírások betartása mellett lehet alkalmazni, és a parancsnok, vagy az S6 részlegvezető hitelesítésével kell ellátni a forgalmi eseménynaplót a jogos használat igazolása érdekében. Az egyedi műholdas eszközök felhasználásának szigorú korlátozására – műholdas telefonokról kizárólag szolgálati beszélgetés kezdeményezhető – nagy hangsúlyt kell fektetni a költséghatékony alkalmazás miatt.

A nemzeti kapcsolattartás további lehetőségét biztosítja az RH rádióforgalmi rendszer, amely szintén tartalékként üzemel az előbbiekben ismertetett összeköttetési formák mellett. A kontingensnél a nagytávolságú RH összeköttetés biztosítására egy darab RF-5200/400 W rádiókészülék üzemel, amely a megfelelő (kiutalt) frekvenciák felhasználásával biztosítja a kapcsolatot. Ez a rádióforgalmi rendszer és a biztosított rádiókészülék nem szervezhető át a hadműveleti híradás kiszolgálására, minden esetben a nemzeti kapcsolattartásra kell, hogy biztosítva legyen. Az eszköz továbbá lehetővé teszi az írásos közlemények továbbítását is a megfelelő kiegészítő berendezéssel.[56] A rádióforgalmi rendszer csak eseti összeköttetést (tartalék) biztosít, ezért a rádióösszeköttetés és a frekvenciák értékelhetősége miatt meghatározott időközönként kapcsolatfelvételt kell létesíteni a tagállomásokkal, amely dokumentálása fontos a későbbi felhasználása érdekében. A rádiók automatikus

52 A videokonferencia a vizuális kommunikáció leghatékonyabb és legköltségkímélőbb válfaja. Lehetővé teszi a közvetlen, interaktív és magas színvonalú kommunikációt egyszerre több felhasználó között. Az MH VTC feladata az MH-n belüli rendszeres videó-telekonferencia kapcsolat kialakítása az MH és HM azon szervezetei között, amelyek rendelkeznek megfelelő végberendezésekkel (kijelölt szervezetek, missziók).

53 „A NATO Irodaautomatizálási Rendszer (NIAR) rendeltetése, hogy védett információcserét biztosítson a NATO és tagállamai felső szintű politikai és katonai vezetése számára; támogassa a katonai vezetést (C2) a katonai műveletek végrehajtása során; valamint elektronikus levelezési és belső használatra szóló web-szolgáltatást nyújtson az arra jogosult felhasználók számára. A NIAR gyakorlatilag a NATO CRONOS rendszerének magyarországi kiterjesztése." [27]

54 STU II: (Secure Telephone Unit); Az STU II végberendezést az Amerikai Egyesült Államok Nemzetbiztonsági Ügynöksége (National Security Agency) fejlesztette ki, amely a '80-as évektől napjainkig biztosítja a biztonságos beszéd alapú összeköttetést. Számos titkosító végberendezések vannak jelen a NATO tagországok hadseregeiben, amelyek képesek együttműködni a szabványoknak megfelelő kialakítás következtében. Ez nagymértékben elősegíti a kommunikációt a többnemzeti műveletekben résztvevő tagországok számára. Ilyen eszköz például a „NATO interoperabilis" ELCRODAT 5-4 berendezés. (Rohde & Schwarz)

55 Az IVSN helyett ma már az „FOC+" rendszert alkalmazzák.

56 A rádiókészülékhez csatlakoztatott számítógéppel és a telepített szoftverrel.

összeköttetés felvételi (ALE: Automatic Link Establishment)[57] üzemmódot is biztosítanak a felhasználásuk során.

A kontingens ideiglenes felszerelési jegyzékében szereplő „hazai SIM kártyás" GSM készülék – amelyet folyamatos bekapcsolt állapotban kell tartani – a hazai kapcsolattartás további eszköze lehet. A készülékeket csak szolgálati összeköttetésre lehet alkalmazni, egyéb felhasználását a parancsnok engedélyezheti.

A híradó és informatikai rendszer egyik eleme az FTP híradás, amely az MH PRT nyílt-, szolgálati-, és magánküldeményeinek továbbítását biztosítja. Az Afganisztánban jelen lévő magyar erők logisztikai ellátására kijelölt szervezet az MH 64. Boconádi Szabó József Logisztikai Ezred. A küldemények a meghatározott rendben kerülnek továbbításra a logisztikai szállításokkal együtt végrehajtva.

Az MH PRT hadműveleti elöljárójával az ISAF RC(N)-el történő kapcsolattartást az ISAF Főparancsnokság (HQ: Headquarters)[58] biztosítja a NATO nyílt és védett híradó- és informatikai rendszerében. Az összeköttetés vezetékes és vezeték nélküli rendszerekben egyaránt kiépítésre került. Az elöljáró által biztosított híradó- és informatikai, információvédelmi eszközök átvételét a HIRIF biztosítja, majd a szakállomány felkészítését, annak ellenőrzését hajtja végre.

Egy lehetséges összeköttetés nyílt NATO IVSN távbeszélő kapcsolattal kerül megvalósításra, amely a magyar rendszer központján keresztül történik. Az előzőekben említett STU II B végtitkosító berendezés felhasználásával titkosított vonalak, illetve internet alapú telefonszolgáltatás (VoIP: Voice over Internet Protocol) áll rendelkezésre a hadműveleti elöljáró irányába. A német elöljáró rádióösszeköttetést is szervezett a magyar tábor irányába, amely PRC-117/F[59] rádiókészülékekkel kerül végrehajtásra. A harcászati műhold-kommunikációs (TACSAT: Tactical Satellite Communications) rádió nyílt- és zárt rendszerben alkalmas hang- és adat továbbítására valamint fogadására, amely a széleskörű igényeket és követelményeket kielégíti.

Afganisztán területén – és más válságövezetben, ahol a NATO jelen van – civil szolgáltatók is megjelentek, akik különböző kommunikációs lehetőségeket, hálózatokat biztosítanak az ISAF erők számára. A csekély helyi kommunikációs infrastruktúra nem volt alkalmas a katonai használatra, így azt nem tudták felhasználni a PRT-k és más jelenlévő nemzetek katonái. Természetesen a befektetők megjelenése nagyobb lehetőséget biztosít a missziós feladatokat ellátó kontingensek számára. Napjainkban az egyik legnagyobb jelen lévő vállalat a THALES[60], aki egy teljesen kiépített hálózattal (FOC+) járul hozzá az ISAF erők vezetés és irányításának biztosításához. A kommunikációs rendszer nagy távolságú és teljes hadműveleti képességekkel rendelkezik, biztosítva az ISAF számára a nyílt- és titkos összeköttetést a vezetési pontok, táborok rendszerbe foglalásával. A THALES és a NATO Konzultációs, Vezetési és Irányítási Hivatala (NC3A: NATO Consultation, Control and Communication Ageny)[61] által aláírt szerződésnek megfelelően a THALES biztosítja az ISAF erők részére a kommunikációs szolgáltatásokat, üzemelteti és karbantartja azt, növeli a hálózati kapacitást a jelenlévő erők megnövekedett számának megfelelően. A 24 órás „Helpdesk" szolgáltatással elősegíti a rendszer magas fokú rendelkezésre állását. A

57 Automatikus összeköttetés felvétel biztosítja a rádió automatikus összeköttetés felvételét egy másik RH rádióval a kezelő személyzet beavatkozása nélkül.

58 A NATO vezetésű misszió Kabulban települő hadműveleti parancsnoksága, amely az afgán kormánnyal, más kormányzati-, és nem kormányzati szervekkel együttműködve vezeti és irányítja az újjáépítési feladatokat, illetve támogatja az ENSZ munkáját a térségben.

59 A Harris PRC-117F egy többsávos rádió, amely lefedi a 30-512 MHz-es frekvenciatartományt. A beágyazott biztonsági megoldások kommunikációvédelmi (COMSEC: Communication Security) és átvitelvédelmi (TRANSEC:Transmission Security) képessé teszik a készüléket, továbbá alkalmas műholdas összeköttetésre, és képes együttműködni katonai és civil rendszerekkel egyaránt. A katonai szabványoknak megfelelő képességekkel rendelkező eszköz hang és adatátvitelt biztosít harcászati műholdas rendszerekben.

60 THALES: Világméretű francia vállalat, amely kommunikációs lehetőségeket, eszközöket biztosít a polgári és katonai felhasználóknak egyaránt.

61 Az NC3A feladata a NATO folyamatos, szakmai tudományos támogatása.

felhasználók (ISAF HQ, RC-k, PRT-k) számára nyílt- és titkosított hang-, adat-, fax-, valamint információs szolgáltatásokat biztosít LOS (Line of Sight)[62] optikai és műholdas kapcsolatokkal. Jelenleg több mint 60 úgynevezett PoP (Point of Presence) (táborok és parancsnokságok) alkotja a hálózatot.

További kapcsolattartási lehetőség a hadműveleti elöljáró irányába a GSM telefonkészülékek alkalmazásával valósulhat meg. A jelenlévő szolgáltatók a Roshan (Telecom Development Company Afghanistan Ltd.) és az AWCC (Afghan Wireless Communications Company), akik biztosítják a hálózatelérést a felhasználók számára. Ez természetesen nem összehasonlítható más, fejlettebb ország (pl.: Magyarország) mobilszolgáltatói által nyújtott szolgáltatásokkal. [28] Az ISAF továbbá a német mobiltelefon hálózatot is használja, amely a T-mobile rendszer tagja.

Az Iridium és Inmarsat eszközök tartalékként felhasználhatók az elöljáróval való kapcsolattartásra, de ezek nyílt összeköttetést biztosítanak. Az Inmarsat műholdas készülék továbbá kiegészíthető STU II végberendezéssel, amely biztosítja a titkosított összeköttetést a végpontok között, és így minősített információk továbbítására is alkalmassá válik. A hadműveleti- és a nemzeti elöljáró irányába számos nyílt és minősített összeköttetés biztosítja a kapcsolattartást az MH PRT számára, amely nagymértékben hozzájárul a kontingens biztonságához és a feladatok végrehajtásának irányításához.

4.2. A magyar Tartományi Újjáépítési Csoport hadműveleti híradása

Az MH PRT műveleti területen végzett tevékenységének híradó biztosítása a feladatok sikeres végrehajtásának alapvető eleme. A műveleti híradás két alapvető összetevője a táboron belüli és a különböző táboron kívüli műveleti feladatok ellátását biztosító híradó- és informatikai rendszer.

A magyar tábor elhelyezési körletének, valamint az őrzés-védelmi feladatainak híradó biztosítása érdekében a letelepített HIK konténerben elhelyezett HICOM-300E távbeszélő központ az alapeleme. A nemzeti- és az ISAF elöljáróval való kapcsolattartásra a helyi GSM telefonokkal történő kommunikáció támogatására biztosított fővonalak mellett, a központ mellékei állnak rendelkezésre a különböző munkahelyek, pihenők és az őrzés-védelem számára. Természetesen a nyilvános telefonkészülékek a személyi kapcsolattartáshoz is a központról biztosítottak. Az esetleges távvezérelt rádió vonalak mellékeit szintén a központ valósítja meg. A táboron belül az elsődleges összeköttetés a távbeszélő központ mellékeinek, és az informatikai hálózatnak (pl. levelezés) a felhasználásával valósul meg. A holland vezetésű PRT által kiépített, tőlük alkalmazásra átvett távközlési elemek kerülnek jelen esetben elsődleges felhasználásra.

A táboron belüli kapcsolattartás továbbá megvalósítható a rendelkezésre álló kisteljesítményű, kézi URH adó-vevő rádiókkal, illetve esti lehetőségként helyi SIM kártyás GSM mobiltelefonokkal. A tábor őrzés-védelmi feladatát ellátó alegység[63] híradó támogatása elsődlegesen vezetékes összeköttetéssel valósul meg. A felállított őrök, EÁP-ok, kapuszolgálatok híradó kiszolgálását a „Panasonic központ" biztosítja, amely a HIK-be kerül csatlakoztatásra. Az őrzés-védelemben résztvevő szolgálati helyek függvényében kell kialakítani a vezetékes híradást. A kisközpont a szolgálati helyen kerülhet elhelyezésre, amely biztosítja – típustól függően – a végpontok csatlakoztatását, ahol a rendelkezésre álló végberendezések kerülnek kihelyezésre.

A PRT a műveletek végrehajtása során Műveleti Csoportokat (MT: Mission Team) hoz létre, amelyek személyi összetétele az adott feladatnak megfelelően változik. Állandó tagja a két fő összekötő és az egészségügyi részleg. A szervezet többi tagja – CIMIC állomány,

62 közvetlen rálátás (például mikrohullámú összeköttetés esetén közvetlen rálátás szükséges az antennák között a kapcsolat megvalósítása érdekében)
63 Őr- és Biztosító század, őr- és biztosító szakaszok

biztosító erők, stb. – a küldetésnek megfelelően kerül kiválasztásra, hogy a tábortól távoli területeken végrehajtott önálló műveletekre alkalmazható csoport kerüljön megszervezésre.

A műveleti feladatok biztosításához kialakításra kerülő híradás az előzőekben leírtak szerint változhat, de minden esetben biztosítva kell, hogy legyen a tábor és a konvoj közötti, a konvojon belüli, a MEDEVAC és egyéb támogató összeköttetés. Fontos alapelv, hogy a híradást a rendelkezésre álló technikai eszközökkel, a kiutalt frekvenciák felhasználásával úgy kell megszervezni, hogy a menetoszlop minden gépjárművében a rádióforgalmi rendszerbe való belépésre alkalmas híradó eszköz legyen. A csoport minden tagjának ismernie kell a rádiók alkalmazását felhasználói szinten, és képesnek kell lennie a megerősítő, illetve a MEDEVAC erők kérésére az erre kijelölt eszköz felhasználásával. A rádióforgalmi rendszabályok betartása és betartatása elengedhetetlen követelmény. A vezető állomás minden esetben a parancsnok, a tagállomások csak indokolt esetben (azonnali közlemény) kezdeményezhetnek hívást. Fontosnak tartjuk továbbá a különböző lát-, és hangjelző eszközök alkalmazását, amelyek az elsődleges összeköttetési formák kiesése esetén a híradó eszközök alternatívájaként kerülhetnek felhasználásra.

A tábor irányába történő összeköttetés elsődlegesen RH, a menetoszlop belső híradásának kialakítása pedig URH rádióforgalmi rendszerek megszervezésével kerül kialakításra. A feladatok végrehajtásának figyelembevételével kialakított rádióhíradás megszervezésért és megtervezéséért minden esetben a híradó- és informatikai részleg felel. A menetoszlop megindulását megelőzően a híradó-technikai eszközök és a rádióforgalmi rendszerek próbája mindig kötelező érvényű, amelyet az S6 részlegvezető, vagy az általa kijelölt személy leellenőriz, majd jelenti a parancsnoknak a tapasztalatokat. A feladat végrehajtása csak ezt követően kezdődhet meg. A frekvencia felhasználás minden esetben az elöljáró (ISAF) által engedélyezettek szerint kell, hogy megtörténjen, az esetleges új igényeket a rádióforgalmi rendszereknek megfelelően az elöljáró szervezet frekvencia-menedzsmentjétől kell igényelni, az előírásokban meghatározott formanyomtatványokkal. A forgalmi eseménynaplók és egyéb rendszeresített okmányok pontos és részletes vezetése alapvető követelmény minden felhasználó számára.

A rádióhíradás megtervezésekor kiemelt figyelmet kell fektetni az együttműködési képesség mellett a földrajzi és éghajlati tényezők negatív hatásaira. Gyakran előfordulhat, hogy a terepviszonyok[64] hatására nem létesül összeköttetés adott esetben még a konvojon belül sem.[65] Fontos a rádiók kimenő teljesítménye is, amely szintén fontos tényező a megbízható összeköttetés megvalósításában. A menetoszlopokban résztvevő gépjárművek, mint például a Hummer (HMMWV 1114) terepjárók vastag páncélborításának köszönhetően életet menthetnek[66], de a rádiók használatát is nagymértékben korlátozhatják. A tapasztalatok több alkalommal is bizonyították, hogy a felhasználásra tervezhető 1W kimenő teljesítményű URH rádiókészülékek (pl.: Kongsberg MRR MH-300-as) nem, vagy nem teljes szélességben biztosítottak összeköttetést a konvojon belül, az előzőekben említett tényezők miatt. A frekvenciák megválasztásánál – ezáltal a rádiók megválasztásánál is – meg kell vizsgálni továbbá az egyéb készülékek, mint a jammer[67]-el történő együttműködési képességeket. Az aszimmetrikus hadviselés egyik jellemző támadási formája a távirányítású bombák alkalmazása a hadszíntéren. Az ellenséges irreguláris erők, terrorista merénylők által gyakran

64 A terepviszonyok nagymértékben befolyásolják a katonai tevékenységeket, a csoportok minden műveletére hatást gyakorolnak. A tagolt, átszeldelt terep meredek völgyoldalakkal, magas hegyekkel, árkokkal, esetlegesen vízmosásokkal hatást gyakorolnak a feladat végrehajtására. A kedvezőtlen terület nem csak a közlekedést nehezíti meg, illetve az esetleges támadások, rajtaütések időbeli észlelését, de a híradást is korlátozhatja.

65 Tóth András, az MH PRT hetedik váltásának híradó- és informatikai részlegvezető-helyettese tapasztalatai alapján.

66 „A Magyar Honvédség Tartományi Újjáépítési Csoport (MH PRT) egyik összekötő csoportja felelősségi területén CIMIC-ellenőrzéssel kapcsolatos feladatot hajtott végre, melynek során helyi idő szerint 11.16-kor Pol-e Khomritól dél-keletre mintegy 80 kilométerre, az Andara völgyben Deh-e-Selah és Banu járás határán támadás érte őket” [29]

67 Elektronikai zavaró állomás/eszköz, amelyet katonáink a missziós műveletek során alkalmaznak a rádió távirányítású bombák működtetésének zavarásához.

alkalmazott házi készítésű robbanóeszközök, távirányítású bombák újragondolt elveket követeltek meg a katonai vezetéstől. A különböző haditechnikai eszközöket gyártó cégek, és a nemzetközi műveletekben résztvevő nemzetek nagy hangsúlyt fektetnek az improvizált robbanó eszközök (IED: Improvised Explosive Device) elleni védelemre. Az IED elleni eszközök feladata, hogy a telepített robbanószerkezeteket felfedi, azokat semlegesíti. Az katonák és a haditechnikai eszközök ilyen irányú védelme nagyon fontos. Az MH PRT-re alaprendeltetéséből adódóan járőrözési, és egyéb feladatai ellátása során, az út mellé telepített IED-k nagy veszélyt jelentenek, ezért fontos, hogy rendelkezzenek a megfelelő zavaró eszközökkel, amelyek biztosítják, hogy a telepített – például az út mellé – távirányítású robbanószerkezeteket (RCIED: Radio Controlled IED)[68] semlegesítsék. Bár Afganisztánban a támadások e típusa nem új megjelenésű az ISAF erői számára, de nagy problémát jelent erőteljes térnyerése, a támadások gyakoriságának növekedése és az eszközök folyamatos fejlesztései. A fejlett jammer eszközök programozhatóak, így biztosítva a saját kommunikációs eszközök zavarásának elkerülését, amely a vezetés és irányítást nagymértékben korlátozná. [30] Ezen blokkoló eszközök alkalmazása fontos eleme az elektronikai hadviselésnek (EW: Electronic Warfare). Az ISAF erők kommunikációjának kiegészítésére felhasználható helyi GSM hálózat elősegítheti, kiegészítheti az összeköttetést a csapatok között, de egyben nagy kockázatot jelenthet, mivel a mobiltelefon hálózatot használják fel az ellenséges erők az IED-k működtetésére.

Látható, hogy a konvojok híradó biztosítása az egyik legérzékenyebb területe a műveleteknek, mert a rajtaütések mellett a robbantási merényletek is hatásosak a többnemzeti erők tevékenységének meghiúsítására. Amennyiben a rádióhíradás korlátozva van (környezeti hatások), a helyi SIM kártyákkal ellátott GSM készülékeket is felhasználhatják az MT-k. A HIK konténer analóg fővonalán telepített, helyi SIM kártyával ellátott GSM adapter biztosítja a konvoj és a tábor közötti kapcsolatot. Az MT mobiltelefonnal történő ellátását a parancsnok szabályozza a résztvevő állomány és a feladat függvényében. A GSM mobiltelefonok használatát nagymértékben befolyásolja, hogy az ország teljes hálózati lefedettsége nem megoldott. Elsősorban a nagyobb települések, főbb útvonalak mentén biztosított az összeköttetés. Amennyiben olyan területen halad át az MT, ahol nincs hálózat, abban az esetben a műholdas eszközök kerülnek felhasználásra. Természetesen a parancsnoknak és az S6 részleg vezetőjének minden esetben meg kell határoznia minden felhasználó részére, hogy melyek azok a készülékek, híradó-technikai eszközök, amelyek alkalmazhatók szolgálati, minősített közlemények továbbítására.

A rádióforgalmi rendszerek tartalékaként más összeköttetési lehetőséget is terveznie kell az S6 részlegnek. A rádiók kiesése esetén alkalmazásra kerülhetnek az Iridium és Inmarsat műholdas eszközök, amelyek kevésbé „érzékenyek” a terepadottságok negatív hatásaira. Amennyiben műholdas híradás kerül felhasználásra hadműveleti feladatok ellátása során, abban az esetben minden résztvevőnek (tábor HIK, és/vagy HDM Ü; a konvoj) rendelkeznie kell műholdas készülékekkel. A táborral történő összeköttetés megvalósítása érdekében minden esetben bekapcsolt, hírváltásra kész állapotban kell tartani az Inmarsat készülékeket, a konvoj esetleges bejelentkezésének fogadása érdekében. Az Iridum műholdas mobiltelefonok szintén tartalékként, de akár fő eszközként is felhasználásra kerülhetnek a műveleti feladatok végrehajtása alkalmával. Amennyiben ez kiadásra kerül az MT-k részére, akkor a tábor területén, a HDM Ü helyiségében, – az Inmarsat eszközhöz hasonlóan – bekapcsolt, hívásfogadásra kész állapotban kell tartani egy Iridium telefont. Az Inmarsat használatát lehetőség szerint kerülni kell a magas költségek miatt, ezért célszerű tartalékként, a lehető legrövidebb információcserére alkalmazni. Az Iridium eszközöket elsődlegesen hálózaton belüli és a helyi földi hálózat felé irányuló hívásokra kell használni.

68 Ezen csoportba tartoznak a rádiófrekvenciás eszközökkel (cellás mobiltelefonok is) vezérelt robbanószerkezetek, amelyek működési elve, hogy a robbanószer mellé telepített valamilyen vevőberendezésre távoli adóról küldött jellel történik meg a detonáció, amelyet a szerkezet használója időzít, a megfelelő időben történő adással.

A mai vezetés és irányítási rendszer alapját képezi a saját erők követését biztosító rendszer (BFTS: Blue Force Tracking System)[69], amely a sikeres feladat végrehajtást támogatja a hadszíntéren, és lecsökkenti a „baráti tűz”[70] általi veszteségeket. A saját erőkről kapott vizuális információkat a haditechnikai eszközökben és a katonáknál elhelyezett rádióadó-egységektől érkező jelek teszik lehetővé, amelyeket elsőként az amerikai erők használtak Afganisztánban. „Az „Operation Enduring Freedom (OEF) Afganisztán-2003” alatt használták először az amerikaiak a BFTS-t harci körülmények között. A dandár szintű számítógépes hálózat a 21. századi erők harcvezetésére, dandár szinten és az alatt (Force XXI Battle Command, Brigade and Below, FBCB2) és a saját erőket követő alrendszer (Blue Forces Tracking System, BFTS) együttese olyan hatékonynak mutatkozott a szárazföldi műveletekben, hogy az „Operation Iraqi Freedom (OIF) Irak-2004” műveletben is alkalmazásra került.” [31]

A többnemzeti műveletekben a BFTS rendszerek alkalmazása nagyon fontos, az együttműködés sikerének egyik alappillére. Egyes NATO nemzetek rendelkeznek saját BFTS rendszerrel, de az afganisztáni hadszíntéren jelen lévő nemzeti rendszerek között nincs meg a megfelelő együttműködés, amely biztosítja a koalíciós erők egymás elleni támadásának elkerülését. A probléma megoldása érdekében került alkalmazásra egy új szolgáltatás (szabvány), amely biztosítja a kétirányú adatcserét a különböző rendszerek között. [32] Az ISAF által alkalmazott rendszert (IFTS: ISAF Force Tracking System) minden résztvevő ország felhasználja, és biztosítja a hadszíntéren jelen lévő erők megjelenítését a parancsnokok számára. Az IFTS egy műholdas kommunikáción alapuló rendszer. Minden IFTS eszközzel ellátott gépjárműről az adatok egy központi szerverre kerülnek továbbításra - amely irányítja az IFTS-t -, majd az továbbküldi az összes terminálnak a hadműveleti területen. A stacioner-, hordozható- és gépjárműbe szerelt eszközök rendelkezésre állnak a résztvevő alegységek és az RC-k számára, így biztosítva az erők nyomon követését. Természetesen az MH PRT is rendelkezik IFTS eszközzel, amely nagymértékben hozzájárul a biztonságos és sikeres feladatok ellátásához. [33]

Az egyéb híradási feladatok csoportjába tartozik a magánbeszélgetések biztosítása a személyi állomány részére. Ezt három helyen kihelyezett nyilvános melléken kerül megszervezésre, megvalósításra. A HM-II. objektum központkezelőjén keresztül lehet a hívásokat végrehajtani az „R” beszélgetések rendje szerint.

Az afganisztáni feladatokban tevékenységet vállaló más magyar kontingensekkel, erőkkel való kapcsolat megvalósítása az együttműködési híradás keretén belül kerül megszervezésre, a felszerelési jegyzékben szereplő eszközök alkalmazásával. Az MH PRT hírközpontban végződtetett MH távhívó fővonalak jogosultak IVSN hívásra, így minden NATO IVSN hálózatban lévő mellék (NATO nemzetektől függetlenül) elérhető. Az ISAF és a Magyar Honvédség más kontingenseivel - mint az MH KFOR, MH Műveleti Tanácsadó és Összekötő Csoport (OMLT: Operational Mentoring and Liason Team) - is megvalósítható a kapcsolat az esetleges együttműködés esetén. [34]

Az MH PRT jelenleg a kilencedik váltásával vesz részt az afganisztáni újjáépítési műveletekben. Az eddigi tapasztalatok szerint a csoportok megfelelően látják el az alaprendeltetésükből adódó feladatokat, amelyek híradó támogatása jól kialakított és megszervezett a többnemzeti jelenlét, az eszközök együttműködési képességeinek nem teljes megléte, valamint a kevésbé fejlett eszközök alkalmazásának esetleges negatív hatásai ellenére is.

69 Az amerikai hadsereg használta elsőként ezt a kifejezést arra a műholdas alapú rendszerre, amely a parancsnok számára ad információt egy kijelzőn a saját erők tevékenységeinek helyéről a hadszíntéren. A „kék szó” a saját erőket szimbolizálja, míg a „piros” az ellenséget jelöli. Ezt a „színkódot”, szimbólumrendszert alkalmazzák a szövetséges erők a térképeken történő egyezményes jelek használatakor is.

70 A baráti tűz (baráti támadás) kifejezés az amerikai hadsereg által használt „friendly fire”-ből ered, amely a saját, vagy szövetséges erők általi vétlen tüzet (támadást) jelenti a saját erőink irányába, amely veszteséget okoz számunkra.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A Magyar Köztársaság NATO nemzetközi műveletekben való részvétele a Magyar Honvédség feladatait alapjaiban változtatta meg. A politikai vezetés a haderőt már az új típusú fenyegetések elleni küzdelemre készíti fel a szövetségesekkel együttműködésben. NATO válságreagáló és béketámogató műveletek keretén belül számos feladatot látnak el a magyar katonák külföldi területeken egyedi vagy alegységekben betöltött beosztásokban. A cikk témájának megfelelően, és a kitűzött célok elérése érdekében a legfontosabb, hasonló rendeltetésű, de különböző feladatokat ellátó alegységeket vizsgáltuk meg jelen cikkben. Az általunk tanulmányozott három térségben jelenlévő magyar katonai erők az ENSZ BT határozatait követően, az Országgyűlés jóváhagyásával kezdték meg a szövetséges kereteken belül vállalt feladataik végrehajtását. Mindhárom térség területén végrehajtott művelet közös pontja, hogy valamilyen fegyveres küzdelem (hadművelet) előzte meg, és ezt követően kezdte meg a NATO a béketámogató műveleteket. Minden esetben a szövetséges erők jelentős része vállalt szerepet az adott ország stabilitásának helyreállításában, így megállapítható, hogy többnemzeti műveletekben való magyar részvétel erőteljes megjelenése várható a jövőben is, amely híradó biztosítása nehezebb feladatot állít a magyar fél számára, így erre nagy hangsúlyt kell fektetnie a vezetésnek.

A híradást mindhárom területen befolyásolta a többnemzeti részvétel, az ország földrajzi jellege, a béketámogató műveletek feladatai, az elöljáróval való kapcsolattartás, a helyi kommunikációs infrastruktúra, a felhasználható, rendelkezésre álló eszközök és az együttműködés igénye. Továbbá fontos megemlíteni, hogy a kontingensek zászlóalj (ezred) méretű erők, és ez összhangban van az MH ÖHD-ban meghatározottakkal, amely zászlóalj szintű erők felajánlását írja elő.

Minden esetben széleskörű képességekkel és szolgáltatásokkal rendelkező híradó- és informatikai rendszer került kiépítésre, amely biztosította a kontingensek vezetés és irányítását. Azonban a felhasználásra kerülő híradó-technikai eszközökből látható, hogy ezek nem mindegyike kerül hazai felhasználásra[71], nem eleme a rendszeresített, az adott alegység híradását biztosító eszközparknak, így a missziós felkészülés során nagy hangsúlyt kell fektetni az állomány híradó kiképzésére. A híradó- és informatikai rendszerek - a civil élethez hasonlóan - rohamosan fejlődnek, amellyel lépést tartani igen nehéz a szűkös költségvetés miatt. Az MH híradó-technikai korszerűsítés nem-, vagy csak részben képes megfelelni gyors fejlesztéseknek. Mindezek mellett az MH számára új képességeket is figyelembe kell venni (például: IFTS, TACSAT), melyek nagymértékben elősegítik a csapatok vezetését a hadszíntéren. A többnemzeti műveleti jelleg az egységes nyelv (angol) használatán kívül meghatározza a felhasznált eszközöket, eljárásmódokat az együttműködés érdekében. A jelenleg használatban lévő, a kontingensek felszerelési jegyzékében szereplő híradó- és informatikai eszközök bár biztosítják a vezetés igényeit, de ezek korszerűsítése, modernizációja és fejlesztése nem hagyható figyelmen kívül. Ilyen fejlesztési irány lehet a feladatokhoz optimalizált (a tapasztalatok alapján), új képességeket nyújtó eszközrendszerek hadrendbe állítása. Ilyen irányt mutat az Iridium műholdas telefonok fejlesztése[72], az Inmarsat eszközök modernizációja[73], de az MH PRT és az MH OMLT által is alkalmazott PRC-117/F is nagy lehetőséget nyújt a katonai felhasználók számára. Véleményünk szerint a fejlesztési tendencia jó irányba mutat, amelyet a nagyszámú béketámogató műveletekben szerzett tapasztalatok elősegítenek. A híradó- és informatikai rendszer megszervezését

71 A külföldi műveletekben résztvevő állomány által felhasznált egyéb eszközök sem állnak rendelkezésre minden esetben az alakulatoknál. (pl.: páncélozott Hummer terepjárók)

72 Iridium NEXT: új generációs készülék, amely nagysebességű hang- és adatkapcsolatot, és számos új szolgáltatást biztosít az IP technológia előnyeivel.

73 Például az Inmarsat új BGAN szélessávú, hordozható, integrált szolgáltatásokat nyújtó műholdas terminálok, amelyek egy időben képesek hang és adatkommunikációra

tekintve új típusú szervezési eljárásokat kell alkalmazni a megnövekedett igényeknek, az új típusú és új szolgáltatásokat nyújtó eszközöknek megfelelően.

A fejezettel kapcsolatos következtetéseim alapján megállapítható, hogy a többnemzeti műveletekben résztvevő kontingensek híradó- és informatikai biztosítása kiemelt fontosságú a csapatvezetés érdekében. Az összeköttetéseknek megbízhatóaknak, egyes elemeinél védetteknek kell lenniük, a parancsnok és törzse vezetés és irányításának konzekvens végrehajtása érdekében.

Az elöljáróval szervezett híradás elsődleges eszköze minden esetben műholdas összeköttetés, amely a nagy távolság áthidalását megvalósítja. Ezen kívül minden, a rendelkezésre álló lehetőségeknek megfelelően felhasználható híradó-technikai eszköz. A hadműveleti elöljáróval való kapcsolattartás megszervezése, és a technikai eszközök biztosítottak voltak a kontingensek részére.

A táboron belüli, a feladatok végrehajtása során alkalmazott, és az együttműködő szervezetekkel történő híradás alapvető eszköze a vezetékes, RH/URH és egyedi műholdas rendszerek, amelyek összetétele a feladatok függvényében változhat.

A híradást több tényező befolyásolja, amelyek műveleti területenként, a többnemzeti egységek és az együttműködők összetételétől függően változhat. A hadműveleti elöljáró frekvenciamenedzsmentjével történő szoros együttműködést követel meg a többnemzeti szerepvállalás, mivel az alkalmazásra kerülő sugárzó eszközök (civil és katonai eszközök egyaránt) egymást befolyásolhatják, zavarhatják.

A C2 rendszerek alkalmazása véleményünk szerint kiemelten fontos területe a válságreagáló műveletek korszerű vezetésnek. Az MH C2 rendszerének egyik alapfunkciója a saját, illetve ellenséges erők, eszközök, harcrendi elemek különböző méretarányú, digitális térképen történő megjelenítése, a felderítési és állapotadatok, parancsok, intézkedések és formalizált jelentések továbbítása, a rendszer elemeinek helyének és állapotának nyomon követése. Az információk átvitelét a járművekbe szerelt rádiókészülékek biztosítják, amelyek – az eddigi elemzéseimre alapozva – elsősorban a földrajzi adottságok miatt, másodsorban az eszközök átviteli sebességének korlátai miatt nem képesek minden esetben biztosítani az időbeni információcserét. Az ISAF műveletekben alkalmazott IFTS rendszerek műholdas összeköttetések alkalmazásával működnek, amelyek az MH C2 rendszerében eddig nem kerültek integrálásra.

FELHASZNÁLT IRODALOM

[1] 55/1999. (VI. 16.) OGY határozat magyar kontingens részvételéről a koszovói békefenntartásban részt vevő nemzetközi erőkben (KFOR), Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 52. szám; 1999. június 16.; p.: 3359

[2] Tóth András: A béketámogató és békefenntartó műveletek híradása /diplomamunka/ ZMNE, Budapest 2004; p.: 28.

[3] Fekete Károly: VSAT rendszerek alkalmazásának lehetőségei a Magyar Honvédség jelenlegi és távlati hírrendszerében, http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/KF_3.html (letöltve: 2009.06.21)

[4] Németh András: A mobil szolgáltatók hálózatainak felhasználása, fejlesztési lehetőségei és alternatív megoldások a katasztrófavédelmi kommunikáció területén (doktori PhD értekezés) Budapest, 2007 p.: 103.

[5] NATO Kosovo Force (KFOR), http://www.nato.int/kfor/structur/nations/placemap/kfor_placemat.pdf (letöltve: 2010.02.26.)

[6] A honvédelmi miniszter 97/2008. (HK 13.) HM határozata a Magyar Honvédség Őr- és Biztosító Zászlóalj ideiglenes katonai szervezet megszüntetéséről, Honvédelmi

Közlöny a Honvédelmi Minisztérium Hivatalos Lapja, CXXXV évfolyam 13. szám (2008. augusztus 18.); p.: 999-1000.

[7] 41/2008. (HK 8.) HM JSZÁT- HM HVKF együttes intézkedés: A NATO KFOR Nyugati Többnemzetű Alkalmi Harci Kötelékben résztvevő Magyar Honvédség KFOR Zászlóalj híradásáról, informatikai támogatásáról és információvédelméről, Honvédelmi Közlöny a Honvédelmi Minisztérium Hivatalos Lapja, CXXXV. Évfolyam 8. szám (2008. május 9.); p.:632.

[8] 1992. évi LXXII. törvény a távközlésről (A távközlésről szóló 1992. évi LXXII. törvény mellékletének 29. pontja), http://www.1000ev.hu/index.php?a=3&param=8925 (letöltve: 2009.05.21.)

[9] Sándor Miklós–Magyarné Kucsera Erika: A zártcélú hálózat forgalmi optimalizálásának problémái, Kard és Toll 2005/3; ZMNE; Budapest, p.: 107. (ISSN: 1587-558X)

[10] 1992. évi LXXII. törvény a távközlésről (A távközlésről szóló 1992. évi LXXII. törvény mellékletének 8. pontja), http://www.1000ev.hu/index.php?a=3&param=8925 (letöltve: 2009.05.21.)

[11] Hóka Miklós: A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO tagországok rádiórendszereinek vizsgálata tükrében (doktori PhD értekezés) Budapest, 2005 p.: 70.

[12] Horváth Ferenc: A frekvenciagazdálkodás feladata és szerepe a Magyar Honvédségben, http://www.hm.gov.hu/hirek/kiadvanyok/uj_honvedsesegi_szemle/a_frekvenciagazdalkodas (letöltve: 2009.01.11.)

[13] Magyar Honvédség Civil-katonai Együttműködési és Lélektani Műveleti Központ: Irak CIMIC kézikönyve Második, átdolgozott kiadás, Budapest 2006. február; p.. 43

[14] 65/2003. (VI. 3.) OGY határozat az iraki válság rendezése érdekében tett erőfeszítésekhez történő magyar katonai hozzájárulásról, Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 61. szám; 2003. június 03.; p.: 4978

[15] 119/2003. (XI. 5.) OGY határozat az iraki válság rendezése érdekében tett erőfeszítésekhez történő magyar katonai hozzájárulásról szóló 65/2003. (VI. 3.) OGY határozat módosításáról, Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 126. szám; 2003. november 05.; p.: 9511

[16] Globális háború közepén? http://www.demokrata.hu/heti-hir/globalis-haboru-kozepen?mini=program-naptar/2009/12/all& (2009.12.21.)

[17] http://www.hm.gov.hu/honvedseg/mhohp (2009.01.23.)

[18] Tóth András: A béketámogató és békefenntartó műveletek híradása /diplomamunka/ ZMNE, Budapest 2004; p.: 49.

[19] 1995. évi LXV. Törvény az államtitokról és a szolgálati titokról, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99500065.TV (2009.06.21.)

[20] Munk Sándor: Katonai Informatika II.; Katonai informatikai rendszerek, alkalmazások Egyetemi jegyzet; ZMNE, Bp. 2006

[21] Magyar Honvédség Civil-katonai Együttműködési és Lélektani Műveleti Központ: Irak CIMIC kézikönyve Második, átdolgozott kiadás, Budapest 2006. február; p.. 44.

[22] Csermely Nóra: Petersberg, http://www.grotius.hu/publ/displ.asp?id=XWRNWH (letöltve: 2009.02.22.)

[23] 78/2006. (HK 16.) HM utasítása az afganisztáni tartományi újjáépítési csoportban résztvevő katonai szervezet létrehozásának feladatairól, valamint a személyi állomány kihelyezésének előkészítéséről és végrehajtásáról, Honvédelmi Közlöny a Honvédelmi Minisztérium Hivatalos Lapja, CXXXIII. Évfolyam 16. szám; 2006. augusztus 10.; p.:1111.

[24] http://www.hm.gov.hu/honvedseg/mh_tartomanyi_ujjaepitesi_csoport (letöltve: 2009.01.11.)

[25] http://www.isaf.nato.int/en/troop-contributing-nations/index.php (letöltve: 2009.05.25.)

[26] MH Tartományi Újjáépítési Csoport (MH PRT), http://www.hm.gov.hu/honvedseg/mh_tartomanyi_ujjaepitesi_csoport (letöltve: 2009.01.11.)

[27] Munk Sándor: KATONAI INFORMATIKA II.; Katonai informatikai rendszerek, alkalmazások; Egyetemi jegyzet; ZMNE Budapest, 2006; p.: 179.

[28] Rajnai Zoltán – Takács Péter: Az afganisztáni missziós híradás tapasztalatai, Kard és Toll 2006/3; ZMNE; Budapest, p.: 31 (ISSN 1587-558X)

[29] Bocskai István, a Honvédelmi Minisztérium szóvivője: RPG-s támadás érte a magyarokat Afganisztánban, http://www.honvedelem.hu/cikk/24/18274/rpg-s_tamadas_afganisztan.html (letöltve: 2010. 02. 15.)

[30] Makk László-Hajdú László: Az improvizált robbanóeszközök alkalmazásáról, Új Honvédségi Szemle LXI. évfolyam 3. szám (2007. március); p.: 5-21. (ISSN 1216-7436)

[31] Hóka Miklós: A csúcstechnológia alkalmazása a hadszíntéren a szoftverrádiótól a nanotechnológiáig, Szakmai szemle; A Katonai Biztonsági Hivatal Tudományos Tanácsának kiadványa; Budapest, 2006/2. szám; p.:76-77. (ISSN: 1785-1181)

[32] Comtech Telecommunications Corp. Receives $2.5 Million Purchase Order Amendment for NATO Force Tracking System, http://comtechmobile.com/pr020607.html (letöltve: 2009.05.25.)

[33] Négyesi Imre: Az információgyűjtés jövőképe (Hadtudományi szemle on-line, I. évfolyam (2008) 3. szám, 95-100. oldal)

[34] Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője (MK KBH Szakmai Szemle 2009. 3. szám, 35-50. oldal, ISSN 1785-1181)

Koncz Bence
maul88@freemail.hu

FREKVENCIATÁMOGATÁS KÉRDÉSEI A TÁBORI HÍRRENDSZERBEN

Absztrakt

Számottevő analóg rádió található a Magyar Honvédség katonai szervezeteinél. Az R-142 rádióállomás négy készüléket tartalmaz, melyek szintén analóg üzeműek. Ezen készülékek fizikai felépítésükből, működési elvükből és modulációs módjukból adódóan bizonyos frekvenciákon nem képesek sugározni. Ezeket nevezzük önzavart frekvenciának. A híradás megszervezésének alkalmával, a frekvenciák elosztásakor nagy hangsúlyt kell erre fektetni. A megkapott frekvenciacsomag, amiből egy katonai alakulat gazdálkodik, tartalmazhat olyan frekvenciát, ami nem használható. Jelen közlemény e problémára kínál megoldást.

People can find several analogue radios in the units of the Hungarian army. The R-142 radio station consists of four radio devices which are also analogues. These devices are can not work on some frequencies coming from their physical structure. We say self jammed for these frequencies. During the organization of the signal service of the army the specialist have to pay attention for it. Every military unit have to get a frequency package. It can contains some frequencies which are unusable.

Kulcsszavak: *frekvenciamenedzsment, R-142 rádióállomás, tábori hírrendszer ~ frequency management, R-142 radio station, field CIS*

BEVEZETÉS

A Magyar Honvédség katonai szervezeteinél üzemelő híradástechnikai berendezések számottevő része azok az analóg elven működő eszközök, melyek a rendszerváltás előtt kerültek rendszeresítésre. Akkor, mint a Varsói Szerződés tagállama kapa őket az akkor Magyar Néphadsereg néven üzemelő szervezet. Használatuk és rendszerben tartásuk pedig még több évig is lehetséges a velük kapcsolatos problémák orvoslása pedig egyre inkább szükséges. A hatékony üzemeltetés érdekében érdemes figyelmet fordítani a hatékony frekvenciatervezésre – mint speciális területre, mert:

- A mai gyakorlat szerint a katonai szervezet számára kiutalnak egy frekvenciakontingenst, melynek fő típusai URH, RH, és a relékhez kapcsolódó folyószámok.
- Napi szinten előfordul, hogy több generációs analóg rádiókat használnak egy szervezetnél és ezekkel együtt kell működni, a szintén rendszerben lévő csekély mennyiségű digitális rádióval.
- A fő probléma, hogy a frekvencia kontingensen belül adott, hogy milyen frekvenciák használhatók, sok esetben a készülék rasztere nem esik egybe a kiadott frekvencia értékekkel, ebből kifolyólag pedig több estben is előfordulhat, hogy nem lehetséges a rádió előírt frekvenciára való behangolása. Pl.: az R-111, 25 kHz-es raszter távolsággal rendelkezik, de ha 1 kHz-enként csupán néhány frekvencia engedélyezett a számára.
- A katonai szervezeteknél, a híradó okmányok kidolgozása során felmerülő hiányosságokra szintén fontos válaszlépéseket tenni.

- Előfordulhat, hogy sem a raszter, sem az üzemeltetési frekvencia tartomány nem teszi lehetővé a hatékony frekvenciamanővereket.
- A hibákat kiküszöbölendő, segíteni kell a hibás rendszerbe illesztések elkerülését.

1. MŰKÖDÉSI ZAVAROK FELVETÉSE, ELŐZETES ELGONDOLÁSOK A PROBLÉMÁK KEZELÉSÉRE

A felbukkanó műszaki probléma abban rejlik, hogy az analóg rádiók jelentős része nagyszámú önzavart frekvenciával rendelkezik, amit általában a kezelők ritkán, vagy egyáltalán nem vesznek figyelembe csakúgy, mint a rendszert szervező személyek.

Nélkülözhetetlen figyelembe venni, hogy egy híradó komplexumon belül telepített analóg rádiók az adott frekvenciakonfiguráció mellett jelentősen zavarhatják egymást (itt beszélünk kölcsönös zavarásról).

1. kép: Az R-142 rádióállomás telepítése
Forrás: A szerző felvétele

A felsoroltak erősítik azt a tényt, miszerint ezen rendszerek hatékony működési feltételeinek kialakítását mindenképpen elő kell segíteni. Egy lehetséges megoldás, hogy a kritikus adatokat közös adatbázisban foglaljuk össze és megfelelő program segítségével az önzavart frekvenciák, valamint a kiadott, de a raszternek nem megfelelő frekvenciák, illetőleg a hibásan megadott frekvenciatartományok kombinációját a mintaprogram által elkerülhetővé tesszük. Ezen kívül, a módszer alkalmazásával a hibás rádióforgalmi adatlapok kiadásának problémája is megoldódhat.

E megoldásnak lényegében a híradó és informatikai főnök munkája hatékonyságát növeli oly módon, hogy az elöljárótól kapott adatok bevitele során megoldhatóvá válik a rádióforgalmi rendszer adatlapjainak precíz, pontos és automatikus kitöltése, illetőleg a hívójelek generálása egy megadott adatbázis alapján. A gyakorlati kialakítás során a legegyszerűbb irodai szoftvereket célszerű felhasználni.

2. A FREKVENCIAMENEDZSMENT ALAPJA

Az egyes frekvenciákhoz a katonai szervezetek bizonyos eljárások útján jutnak hozzá. Ennek fő szabályait alapvetően két rendelet határozza meg. A frekvenciaigénylés folyamata is keretek között folyik, melyeknek alapját jogi meghatározások alkotják.

A 346/2004. (XII. 22.) Korm. rendelet, amely magában foglalja, az elosztási eljárás felépítését, és az MH feladatait. A másik a 29/2005. (VII. 27.) HM rendelet, ez a frekvenciakijelölés és a rádióengedélyezés folyamatait taglalja pontosan.

Abban az esetben, ha a kapott frekvencia nem alkalmazható, de a rendszer fennmaradása érdekében a készüléknek üzemelnie kell, fennáll a jogszabályok megsértésének veszélye. Ennek elkerülése csak pontos és helyes frekvencia kiosztással lehetséges, valamit a folyamatos ellenőrzéssel. Az egyes rádióállomások dokumentumai pedig pontosan ezt a célt szolgálják, tehát a nyilvántarthatóságot és a visszaellenőrizhetőséget biztosítják az állomás számára.

3. AZ OKMÁNYRENDSZER KAPCSOLATA A MENEDZSMENT TEVÉKENYSÉGGEL

A Magyar Honvédség katonai szervezeteinek híradó és informatikai szakalegységeinél megtalálhatóak azok az okmányok, melyek a rájuk jellemző feladatból és haditechnikai felszerelések használatából kifolyólag, az elvárható szintű működéshez szükségesek.

A különböző típusú rádióállomások és készülékek is egyenként rendelkeznek olyan dokumentumokkal, amelyek segítségével az elöljárók, parancsnokok és a többi, ellenőrzésre jogosult személy és szervezet figyelemmel tudja kísérni a technikai felszerelések működését, és a konkrét feladat végrehajtások lezajlását.

Az okmányrendszerben véltem felfedezni egy hiányosságot, ami észrevételem szerint nagyban csökkenti a frekvenciamanőverezések biztonságát. A Rádióforgalmi Rendszer adatlapja a hívójelek közül csak egy tartalék hívójellel rendelkezik, amíg tartalék frekvenciából tizenkettővel.

Ezt az adatlapot és ez által a rendszert is módosítani kell a meglátásom szerint, mivel ha tizenkettő nem is, de négy tartalék hívójel mindenképp elfér a rendszer adatlapján nagyobb szerkezeti változtatás nélkül. Ezek egyesével, következetesen összerendelésre kerültek az egyes tartalék frekvenciákkal. A változtatások alkalmazása a rendszer biztonságosabbá tételét eredményezik, mivel ha egy csatornaváltást hajt végre a kezelői állomány, akkor másik tartalék hívójelen jelentkezik be, ezáltal a tevékenység nehezebben felismerhető a zavarást, vagy lehallgatást folytató rádióelektronikai felderítők számára.

4. TECHNIKAI ANOMÁLIÁK

Létezik azonban egy másik probléma is, amely véleményem szerint összetettebb mint az előbbi. Ez az egyes készülékek felépítéséből és az alkatrészek fizikai tulajdonságaiból következik.

Egyes frekvenciák úgynevezett önzavarással fedettek. Az egyik készülék, ahol ez számításba jöhet, az R-123 MT. Ezen berendezés alapfrekvenciájának kiválasztásakor egy megbízható rádiós kapcsolat megteremtésekor az alábbiakat tanácsos szem előtt tartani:

- A készülék adója olyan mellékfrekvenciákat is sugároz az üzemi frekvencián kívül, amik növelhetik a különböző rádiókészülékek egymás közti zavarását.
- Káros moduláció jelenik meg az adó némely frekvenciáján.
- A rádiókészülék vevője az üzemi frekvencián vett információn kívül befogja a reagálási átteresztő csatornán kívül a téves csatornákon beérkező információkat, ez a jelenség is növeli a rádiók közötti zavarást.
- A rádió vevőkészülékében önzavaró frekvenciák fordulnak elő, melyek károsodásokat okozhatnak a vevőben.

Alapvetően a mellékfrekvenciák kisugárzásának okai a nem lineáris elemek, azaz a teljesítményerősítő jelleggörbéjének nem lineáris mivolta, valamint a kétszerező üzem a

rezgéskeltőben. Ennek eredményeképp a vevő kimenetén nem csupán az üzemi frekvencia felharmonikusai, hanem a rezgéskeltő felharmonikusai is megjelennek. Ezek pedig együtt jelentkeznek majd a teljesítményerősítőn.

A másik rádiókészülék, aminél erre a jelenségre számítani lehet, az R-130-as berendezés. Lényeges megjegyezni, hogy ez rövidhullámon képes forgalmazni. Elsősorban a szárazföldi csapatok kommunikációját hivatott támogatni, így elsősorban a lövész, páncélos és felderítő alegységeket, de képes kapcsolatot létesíteni bármely olyan eszközzel, amellyel egy fajta modulációs rendszerben, illetve frekvenciasávon üzemel. Üzemi frekvenciájának kiválasztása során nagy hangsúlyt kell fektetni a rádióhullámok terjedési viszonyain kívül arra, hogy a berendezés bizonyos frekvenciákon nem képes rendeltetésszerűen működni, ezeket nevezzük önzavart frekvenciáknak. Továbbá olyanok is vannak, amelyek adáskor káros sugárzásokkal járnak együtt, tehát a rádióállomáson belül kölcsönös zavarást okozhat.

2. kép: Az R-142 rádióállomás belső felépítése
Forrás: A szerző felvétele

4.1. Problémakezelési metodika

Ezen műszaki sajátosságok szervezési problémákat is fölvetnek. Ezért hoztam létre egy mintaprogramot, amely ennek támogatására jött létre. A program a Microsoft Office Excel 2007 alapján készült, mert a Magyar Honvédség szinte mindegyik szervezeténél ezt, vagy valamelyik másik verzióját használják.

A tervezés folyamán egy olyan irodai algoritmus létrehozása volt a cél mely képes:

- A táblázatba rendezett önzavart frekvenciák tárolására, ezáltal egy adatbázist létrehozni.
- Ennek alapján, felismerni és jelezni a szoftver kezelőjének a beírt frekvencia helyességét.
- A rádióforgalmi adatlap tárolásával elősegíteni a keletkezett információk beillesztését a rendszerbe.
- Nyomtatási lehetőséget biztosítani a rádióforgalmi adatlap részére.
- A már eltárolt adatbázist bővíteni, (esetleg másik rádiókészülékek adataival).
- További (a Microsoft Office Excel 2007 függvényeit alapul vevő) funkciókat befogadni.

Részleteit tekintve, a felsorolt követelmények teljesítéséhez részletes és hierarchikus vizsgálat szükséges. Nagy figyelmet kell fordítani először is a frekvencia sávok különbségére. Ezen értsük a rövid és ultrarövid hullámokon forgalmazó rádiókat, valamint

ezen túl a komplexumon belül megtalálható készülékek forgalmazási sávjait, ha van ilyen, pl.: R-142 M/G esetén.

A fő funkciók eléréséhez, első lépésként, az önütő frekvenciákat táblázatba foglaltam. Ezt a továbbiakban, a szövegben adatbázisnak fogom tekinteni. Továbbá ki kell szűrni, azokat a frekvenciákat a központilag megadottakból, melyek önzavarással fedettek vagy nem felelnek meg az eszköz raszter távolságának, esetleg a frekvencia tartományának.

A mintaprogram képes felajánlani egy frekvencia csomagot a felhasználó számára abban az esetben, ha valamely általa tartalmazott folyószám kerül beírásra, elkerülendő, hogy zavarják egymás működését az egyszerre működtetni kívánt rádiókészülékek.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A jövőben mindenképp érdemes foglalkozni mind a felvetett problémával, mind a továbbfejlesztéssel. A digitális üzemű rádiók, bár jelen vannak a Magyar Honvédségben, viszonylag lassan kerülnek elterjedésre, ezért az analóg készülékek használatával még évekig számolni kell. Ebben az esetben pedig létfontosságú a kellő alapossággal megtervezett rádióforgalmi rendszer.

Jelen közleményemben közzé tett javaslataim – megítélésem szerint – elősegíthetik a híradás és informatika megtervezésével foglalkozó törzsállomány, valamint a szervezési tevékenységet végrehajtó szakállomány munkájának hatékonyságát.

FELHASZNÁLT IRODALOM

[1] 1993. évi LXII. törvény

[2] 29/2005. (VII. 27.) HM rendelet

[3] Az R-142 Rádióállomás kezelési szakutasítása

[4] HÍR-3 rádióforgalmi szakutasítás

[5] 346/2004. (XII. 22.) Korm. rendelet

[6] R-130M adó-vevő készülék műszaki leírása és kezelési szakutasítása / [közread. a] Honvédelmi Minisztérium (1983)

Paráda István
paradaistvan@gmail.com

A NATO-BAN HASZNÁLT MŰHOLDAS ANTENNARENDSZEREK

Absztrakt

Véleményem szerint fontos dolog a NATO missziókban használt antennarendszerek tulajdonságainak bemutatása. Jelen közleményben megismerhetjük a misszióban szolgáló katonáknak a műholdas feladatokkal kapcsolatos tevékenységeinek nehézségeit.

In my opinion the most important task of mine is to represent the properties of antenna systems used in NATO missions. We can get to know the difficulties of the satellite tasks of the soldiers serving in missions.

Kulcsszavak: *híradó és informatikai rendszerek, információtechnológia, műholdas rendszerek ~ CIS, IT, satellite systems*

BEVEZETÉS

A NATO[1] műholdas kommunikációjának követelményei katonai szempontokból, igényekből erednek. Ezek a lejegyzett feltételek főleg a mobilitás, a könnyű össze- és szétszerelhetőség, valamint a rendszer gyors telepítése irányában körvonalazódnak ki. Ezek az igények a csapatok gyors és jobb manőverező képessége miatt alakultak ki. A NATO-ban jelenleg három antennarendszert használnak a műholdas kommunikáció biztosítása érdekében.

Az első az úgynevezett TSGT (Triband Transportable Satellite Ground Terminals), magyarra fordítva a Háromsávú Hordozható Terminál. A három hordozható antenna közül méreteit tekintve ez a legnagyobb, ebből adódik a nehezebb, valamint időigényes telepítés.

A második a DSGT (Deployment Satellite Ground Terminals), ami a Telepíthető Műholdas Terminálok névre hallgat.

A harmadik pedig a BBSST (Bi-Band Satellite Suitcase Terminals), amit magyarosítva legjobban a Kétsávú Műholdas Terminálokra lehetne lefordítani.

Ezeket az antennarendszereket civil cégek biztosítják, illetve szolgáltatják. Követelményeiből rájöhetünk arra, hogy ilyen kommunikációs összekötő berendezéseket főként a missziós övezetekben használnak. A missziókban a NATO jelenleg cseréli, illetve már lecserélve a civil cégek által biztosított könnyen mozgatható antennarendszereket használ. 2001-ben a NATO már civil cégek bevonásával üzemeltette antennarendszereit és biztosította az információ összeköttetést a békefenntartó erőknek Koszovóban, Macedóniában és Albániában (KFOR[2]) valamint Bosznia Hercegovinában (IFOR[3], SFOR[4], EUFOR[5]). 2006 és 2009 között a cégek összesen 21 telepíthető műholdas földi terminált terveztek és szállítottak el a NATO Konzultációs, Vezetési és Irányítási Ügynökséghez, így az nem meglepő, hogy az Afganisztáni (ISAF[6]) illetve Iraki missziókban is ezek az antennarendszerek biztosítják a folyamatos információcserét.

1 NATO - North Atlantic Treaty Organization - Észak Atlanti Szerződés Szervezete
2 KFOR – Kosovo Force – Koszovói Erő
3 IFOR – Implementation Force – Végrehajtó Erő
4 SFOR – Stabilization Force- Stabilizációs Erő
5 EUFOR – European Union Force – Európai Uniós Erő
6 ISAF – International Security Assistance Force - Nemzetközi Biztonsági Támogató Erők

A missziókban a katonai antennarendszereket korlátozott vagy nem létező infrastruktúrával rendelkező területekre kell telepíteni, ebből következően a rendszereknek strapabírónak kell lenniük a folyamatos igénybevétellel kapcsolatban. Ezen felül, meg kell felelnie a terep, illetve éghajlati viszonyoknak is.

1. MŰHOLDAS KOMMUNIKÁCIÓ ÁTTEKINTÉSE

1.1. Történelem

A műholdas kommunikációt a rakétaelmélet alapozta meg, ami Konsztantyin Eduardovics Ciolkovszkij orosz tudóstól ered. Az orosz matematikus már azelőtt egy űrállomás és folyékony üzemanyaggal hajtott rakéta tervein gondolkodott mielőtt az ember megkezdte volna első repülését.

Ezt követően, 1945-ben egy angol író Arthur C. Clarke vetette fel a mesterséges műholdak indítását.

1957. október 4-én bocsátották pályára az első műholdat a Szovjetunióba, Bajkonurból R-7-es rakétával. A Szputnyik 1 névre hallgató műhold alakja gömb és átmérője 58 cm volt. Tömege mindössze 86,3 kg. Az oroszok által pályára állított műhold egyrészt sokkolta az amerikaiakat másrészt a hidegháborús verseny miatt arra késztette őket, hogy fontos lépéseket tegyenek az űrkutatások terén. Miután az Amerikai Egyesült Államok egy amerikai műhold pályára állítási tervet írt elő decemberre az oroszok sikeresen végrehajtották a Szputnyik 2 fellövését. *A*z Egyesült Államoknak kudarcokat kellet megélnie majd újabb tervvel kellett előállnia. Explorer néven munkába fogtak, majd 1958. január 31-én sikeresen pályára állították az Explorer 1 műholdat, ami a Föld mágneses kisugárzási övét fedezte fel. A program ezután sikeresen folytatódott és 1958. október 1-jén megalakult a NASA[7]. Ezek után elkezdődtek az űrutazások, azaz az űrhajózás.

1.2. Műholdpályák

Pályatípusok:

- Kör alakú:
    1) Alacsony pályás (LEO);
    2) Közepes pályás (MEO);
    3) Geo stacionárius (GEO).

- Elliptikus alakú.

Alacsony pálya: LEO - Low Earth Orbit

Magasság: 500-2000 km. Az Irídium[8] és GLOBAL STAR[9] rendszer is ilyen pályán mozog.

Előnyei a kis csillapítás, könnyű jelfoghatóság, valamint a kicsi késleltetési idő. Hátrányai közé sorolható a rossz lefedettség, a gyors mozgás, ami a műhold antennakövetését is megköveteli, illetve a kisebb látótér miatt a műholdaknak kommunikálniuk kell egymással.

7 NASA - National Aeronautics and Space Administration - Nemzeti Légügyi és Űrhajózási Hivatal
8 Irídium – 66 műholdból álló alacsonypályás műholdrendszer.
9 GLOBAL STAR – alacsonypályás műholdrendszer

Közepes pálya: MEO-Medium Earth Orbit

Magasság: 2000-35800 km. Egy köztes pályának is hívhatnánk hisz megpróbálja egymásba olvasztani a LEO és a GEO előnyeit. Elsődlegesen navigációs feladatokat lát el.

Előnyei között találhatjuk, hogy lefedi az Északi és Déli pólust, LEO-hoz képest jobb a lefedettsége és ezen a pályán nem léphet fel túlzsúfoltság. Viszont magassága miatt megnő a késleltetési idő (80ms) és a pályaveszteség (200dB).

Geostacionárius pálya:

Magasság: 35,786 km. Az irányított pálya a föld egyenlítője fölött helyezkedik el, olyan periódussal, ami megegyezik a föld periódusával és a pálya különbség megközelítőleg nulla. A föld felszínéről tekintve a geo stacionárius műhold mozdulatlannak tűnik az égen. Tehát úgy is mondtatjuk, a műhold a Földdel együtt forog. Előnyei hogy rögzített antennával tökéletesen lehet fogni a jelet. Azonban itt fellép a túlzsúfoltság, illetve a késleltetési idő és a pályaveszteség is jelentősen megnő.

Elliptikus: HEO-High Earth Orbit

A magas elliptikus pályákon a műhold csak pár percen át látható egy átvonulás közben, hisz a Földtávolban (a Föld felszínétől akár 40000 km-re is) lassan keringve nagy területen biztosítanak lefedettséget, viszont a Föld másik oldalán gyorsan áthaladnak (a Föld felszínétől pár száz km-re). Például Ellipso rendszer.

2. KÉTSÁVÚ MŰHOLDAS TERMINÁL

Méreteiből és egységeiből adódóan korlátozott műholdas csatornát képes használni. Ez a rendszer kettő frekvenciasávos összeköttetést tesz lehetővé, attól függően, hogy milyen kültéri egységek kerülnek telepítésre.

1. kép

2.1. Kültéri egységek

- motorizált antenna és a hozzátartozó egységek (a 90º-os jelszétválasztó, és a csőtápvonal nem külön foglalatba van helyezve, hanem az antennára van felszerelve.)
  Az ultra-könnyű Vertex RSI 1,2 m-es gyorsan telepíthető motorizáltantennát (QDMA) globális Ku sávos adás és vétel céljából tervezték. mozgási ’síkja’ van. A

vízszintes irányszög (azimut) és a függőleges irányszög (eleváció, dőlésszög,) tengelyeket egyaránt a kábelrögzített egység irányítja.

- felkeverő és erősítő egység
  A felkeverő rendszer a modem 10 MHz-es frekvenciát használja, mint jelet, hogy átkonvertálja az L sávú frekvenciát a műhold frekvenciájává, X sávba.
  A felkeverő erősítőnek külső tápellátása van. A felkeverő erősítőnek van egy helyi oszcillátor frekvenciája. Ezt használja, hogy az L sávot műholdfrekvenciává konvertálja.

- lekeverő és erősítő egység
  Alacsony zajszintű konverter, aminek a feladata az antennáról érkező jelek erősítése és lekonvertálása a műholdvevő által használt frekvenciára. A vételi frekvencia lehet Ku vagy X sáv ezt L sávba lekeveri a helyi oszcillátor frekvencia által. Az LNB-t[10] a modem táplálja (12V-tól 24V-ig).

- antennavezérlő egység
  Az antennavezérlő alrendszer gondoskodik a manuális és automatikus műhold antennakövetésről. Ez magába foglalja a vivő frekvenciakövető vevőkészüléket, az antennairányító egységet, az azimut és eleváció optikai forgásszög érzékelőt, a vízszintes irányszög (azimut) és függőleges az eleváció mozgatás kábelvezérelt motorját, az elektronikus tájolót és az elektronikus dőlésszög mérőt.
  Három mód:

    - Lépés: a pozíciós adatokat lejegyzik egy táblázatba és időközönként frissítik;
    - Memória: a táblázatból származtatott adatok alapján végzik a követést;
    - Kereső: a műholdjel elvesztésénél egy algoritmus használatával újrakeresi.

2.2. Beltéri berendezés (IDU)

- Switchek
  A beltéri modem konténerébe van beépítve. Ez biztosítja a hálózati összeköttetést a telepített berendezések és a főhálózat között.

- GPS[11] forrás
  Mind a modem mind a lekeverő berendezések működéséhez szükséges egy referenciajel.
  A referenciaforrás a 10 MHz frekvenciát a GPS-ből vett jelből állítja elő. Ennek feladata a vevő oldali berendezések szinkronizációja.

- FO[12] modem
  Két fontos funkciót lát el. Kettő csatlakozója van az egyik az adatforgalom támogatására szolgál.A másik csatlakozóján a LAPTOP optikai szálon való összeköttetését teszi lehetővé, azaz összeköti a beltéri egységgel.

10 LNB - low-noise block converter – lekeverő erősítő
11 GPS - Global Positioning System - Globális helymeghatározó rendszer
12 FO modem – Fiber Optic modem – Optikaiszálas modem

- Modem
  Támogatja a különböző modulációkat. Legfontosabb funkciója hogy a digitális jeleket modulokra bontja és egy fokozaterősítő segítségével és a konténerbe továbbítja az adatokat. Viszont az érkező frekvenciajelet, de modulálja. Különböző hibajavítási funkciókkal is rendelkezik melyekkel a lényegesen alacsonyabb jelszint mellet is azonos minőségű (bit hibaarányú) összeköttetést lehet biztosítani. A bemenő és kimenő frekvencia L sávban kb. 1200 MHz. A lekeverő erősítő tápellátását is a modem biztosítja.

A rendszer összesen négy dobozból áll, ami javítja a manőverező képességet, a gyors mozgást missziós illetve konfliktus helyzetek során. Az egységek összekapcsolására koax valamint csőtápvonal rendszert használnak.

3. TELEPÍTHETŐ MŰHOLDAS TERMINÁLOK

A DSGT antennarendszer csak X sávú működést tesz lehetővé.

2. kép

Az antenna tányér a fejegységgel egy Low Passive Inter Modulationnal lett megtervezve és tesztelve, ami a nemkívánatos melléktermékként keletkező rádiófrekvenciás jeleknek, zavaroknak a kiszűrését jelenti. A rendszer magába foglal egy azimut meghatározót és egy dőlés rendszert, ami képes gyors műholdkeresésre.

Az antenna egy automatikus vezérlő és követő berendezéssel van felszerelve, ami megengedi a rendszernek a műhold kapcsolat tartását normális üzemelés alatt.

3.1. Kültéri berendezései

- Antenna:
  Az antenna egy 2,4 m-es könnyű antenna, amely szállítás céljából szétszedhető. Az antenna rendszer magába foglal, merevítőt, egy offset–tengelyű tányérral támogatott alumínium talapzatú törzset, amely kompatibilis a különféle felszerelt fejegységekkel a közös csatlakozóponton.

- Adó alrendszer:
  A Vertex 125 Watt-s állandó teljesítményerősítője (SSPA-je) az antenna központi fejtartójára van felszerelve. Az SSPA berendezés szolgáltatja a jelet, amely a beépített felkeverő erősítő (BUC) által van konvertálva, hogy átalakítsa a sugárzó jelet az L sávból Az X sávba, mivel a modemből érkező L sávú jelet a műhold által

is használható X sávú jellé kell átalakítani. Az SSPA kettő ventillátorral van felszerelve, ami bemeneti levegő és a kimeneti levegő keringetéséért felelős.

- Vevő alrendszer:
  Az LNB[13] lekonvertálja és erősíti, a rádió frekvencia jelet mielőtt ezt megkapja a modem, L sávon koax kábelen keresztül. Az IFL panel biztosítja a hibajavító lehetőségeket és a tesztelés hozzáférési pontját.

- Antennavezérlő alrendszer
  Az antennavezérlő alrendszer biztosítja a műhold kézi és automatikus antennakövetését. Ez áll egy követő vevőből, egy antennavezérlő egységből, Azimut és eleváció szenzorból, azimut és eleváció motorból, egy Flux Gate tájolóból és egy dőlésszögmérőből. A rezolver végzi az azimut szög, a tájoló pedig az elevációs szög érzékelését.

- GPS forrás:
  A frekvencia jel alrendszer biztosítja a 10 MHz frekvenciajelet és az időjelet a DSGT felszerelés számára. Szintén a vevő oldali berendezések szinkronizációjáért felelős.

- Kiegészítő rendszer:
  meteorológiai állomás: Az időjárás állomás méri a szél sebességét és levegő hőmérsékletét. A szenzorok biztosítják a vezeték nélküli kapcsolatot egy benti adat regisztráló berendezéssel, amely figyelmeztetést ad, amikor a szél vagy hőmérséklet az előre meghatározott érték fölött van.
  villámhárító rendszer: Thompson Lightning A571.
  jégtelenítés: A fejegység fagyásgátló egy 200 Wattos fűtőellenállásból, ami össze van kötve a fejegység tartóval és egy egyszerű kapcsoló vezetékből áll.

3.2. Beltéri berendezései

- Modem:
  Megengedi az egyidejű átvitelt és fogadást a 6 duplex (kétirányú) hordozón, valamint csatlakoztatja és szinkronizálja az időzítő jelet 10 MHz külső frekvencia által, amit a DSGT biztosít. Frekvenciaosztásos többszörös hozzáférést (FDMA) biztosít, viszont egy csatornaszállító (SCPC) funkciókkal is rendelkezik valamint az E1 időréses
  2 Mbit/s csatornát is fel tudja bontani.

- Teljesítmény:
  A nem megszakítható tápellátás (UPS) MGE Pulsar Extreme 3200 biztosítja az AC (egyenáramú) teljesítményt az összes DSGT alkatrésznek normális működés esetén (a jégtelenítő kivételével). Ezeket Az UPS-eket a missziók alatt a NATO nyújtja.

A DSGT 13 szállítható dobozból áll. Az egységek összekapcsolására koax valamint csőtápvonal rendszert használnak. A rendszer csőtápvonal része, ami az SSPA-t csatlakoztatja a fejegységhez,kétfajta: merev és rugalmas beleértve a szűrőt is.

13 IFL - Interfész Facility Link - Inter fész eszköz összekötő

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A fenti műholdas antennarendszerek véleményem szerint minden magas feltételnek eleget tesznek, ami megköveteli a pozitív véleményalkotást. A rendszereket főleg katonai szempontból alkalmasnak tartom a feladatok elvégzésére, hisz számos viszontagság ellenére tökéletesen helyt állnak. A missziókban lezajló időjárási viszontagságoktól függetlenül, terepviszonyoktól nem vagy csak nagyon nehezen korlátoltan alkalmazhatóak. Katonai szempontból a könnyű össze és szétszerelés, azaz a gyors mozgathatóság fontos, hisz szállítása rendkívül egyszerű már a méreteiből is adódóan, valamint az alkatrészek precíz és kis helyet foglaló dobozokban kerülnek elhelyezésre, ami a transzportálási feltételeket könnyíti meg. Erről az oldalról megközelítve ezek az antennarendszerek a legalkalmasabbak egy harci körülmények közötti üzemelésre.

FELHASZNÁLT IRODALOM:

[1] http://www.milsatmagazine.com/cgi-bin/display_article.cgi?number=1739128626 Focus... Operational Communications By Craig Harrison, Sales Support + Business Manager, Vizada Networks July 2010

[2] http://www.mult-kor.hu/cikk.php?id=18485 Amerikai presztízsveszteség volt a Szputnyik fellövése 2007. október 4. 15:00

[3] Iványfalvi Attila hallgató: A műholdak katonai alkalmazásának lehetőségei a szárazföldi csapatok harcában, hadműveleteiben és békeműveleteiben Budapest 2004

[4] (cache:DDRMLIUtHR0J:www.mht.bme.hu/~seller/Adaptív/Jegyzet/7fejezet.doc antenna típus {2010 09 29}

[5] https://segoviaip.tms.hrdepartment.com/cgibin/a/highlightjob.cgi?jobid=97&referrer=95&site_id=148&view_language=en-US Copyright 2009, Segovia {2010. 10.01}

[6] http://cryptome.org/eyeball/afpak-comms/afpak-comms.htm cikk September 7, 2009 kép: 6/3/2009

[7] DSGT Operator Training by VIZADA networks

[8] BBSST Operator Training by VIZADA networks

Tibor Farkas – Erik Pándi – Szabolcs Jobbágy – András Tóth
farkas.tibor@zmne.hu – pandi.erik@zmne.hu – jobbagy.szabolcs@zmne.hu – toth.hir.andras@zmne.hu

ORGANIZATION OF THE COMMUNICATION AND INFORMATION SYSTEM SUPPORTING COMMAND AND CONTROL IN THE LIGHT OF CRISIS RESPONSE OPERATIONS OF THE HUNGARIAN DEFENCE FORCES[1]

Absztrakt

Cikkünkben áttekintjük a válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében témájú kutatási tevékenységünket.

The article provides an overview of our research activity about the programme organization of the communication and information system supporting command and control in the light of crisis response operations of the Hungarian Defence Forces.

Kulcsszavak: *híradó és informatikai rendszerek, C2 rendszerek, tábori híradó- és informatikai rendszerek, információtechnológia, válságreagáló műveletek ~ CIS, C2, field CIS, IT, light of crisis response operations*

1. INTRODUCTION (DEFINITION OF THE SCIENTIFIC PROBLEM)

In order to ensure the success of international operations, the ongoing process of restructuring in the Hungarian Defence Forces (HDF) is practicing major influence on the quantity and quality of the communication and information equipments, on the organizing and planning processes, and on the staff as well.

The new capabilities, challenges and management needs that we must be met, are identifying the new directives of modernizations. As a result, new principles and procedures should be based on the modern organization and planning process of the communication and information systems (CIS).

Only small parts in the international operations currently used CIS technical equipments is suitable for the modern support of command and control (C2), because they are outdated and inadequate to ensure the new capabilities. The unique solutions, which are used by the military leadership in international operations, don't ensure the establishment of such kind of complex CIS which support in full spectrum the crisis response operations.

To achieve this, it's necessary to examine all the skills, process and organizational factors, which provides for the Hungarian Army to develop the new methods of CIS which is in match with the new warfare precepts.

1 This paper was supported by the Bolyai János research scholarship of the Hungarian Academy of Sciences

2. RESEARCH OBJECTIVES

- To analyze and examine the principles and system activities of NATO's crisis response operations;
- To determine the general operational challenges, capabilities that are define the HDF's development trends, particularly the CIS;
- To formulate the communication and information support of the crisis response operations;
- To present and to analyze the communication and information support of the HDF's multinational operations;
- To determine the capabilities, requirements, and different factors that are affecting the organization of modern CIS in multinational crisis response operations;
- To propose a possible conceptual process of CIS planning.

3. RESEARCH METHODS

- We have drove a literature examination and literary research on the area of literature being attached to the topic;
- We have studied the different laws, decisions and measures related to the HDF's crisis response operations;
- We have prepared consultations with professionals who operated in multinational operations;
- We have examined the organizational principles considering my experiences in international professional exercises;
- We have analysed and I've drew conclusions from the abilities and organizational procedures of the present CIS;
- We have determined a possible organizational principle based on the strength of the organized knowledge, on the part of inferences, and on the capabilities and factors which affect the CIS.

4. THE STRUCTURE OF REPORT

In the first chapter we analysed the basic principles of the multinational crisis response operations, and we examined the general operational capabilities and requirements of the participant forces in NATO CROs in the mirror of Summit Meetings. Based on the particular ones we examined the national developments insuring the capabilities and the tasks of the HDF. According to the results we defined CIS as a supporting system of the crisis response operations.

In the second chapter we described those CROs, in which the HDF is (was) participating. We studied political and legal backgrounds, the force composition and its tasks. We

examined the structure of the communication and information support, the applied devices, connections. According to the principle of information connections We did the analysis of CIS.

Based on the first two chapters, in the third chapter we defined the professional requirements and influencing factors which are practising effects on the process of organizing info-communication systems. Based on the summarised inferences, we presented a mechanism for the organizing a complex CIS that support the multinational operations.

The final part implies the important recommendations, the considerations and the deductible conclusions, scientific results.

5. CONCLUSIONS

- Based on the international and domestic experiences we stated, that it is necessary to create small-sized forces with multi-functional capabilities (with the supplement of civil abilities), equipped with modern military technical devices, which are fit to the complex operational requirements and to command needs. These forces are able to liquidate the international conflicts and to the domestic applications equally, and according to the ongoing requirements it could be developed with relatively small costs;

- Based on the general operational capabilities and claims we confirmed that the definition of CIS used by the HDF doesn't imply those complex characteristics (because of the equipments and theirs capabilities) that the info-communication systems of the CRO include;

- By analyzing of the examined and introduced communication and information support of the HDF's multinational operations we drew the conclusion, that the planning and organizational methods of CIS include a complex process, which has to consider the factors of the cooperating nations, of the specialized tasks and of the mission area;

- In the interest of the support of the commanding leadership, it is necessary to provide to process and to transmit the optimal information which are expanding on all areas and on all subtasks. In the interest of this we emphasized all the requirements, capabilities and other factors which appear through the multinational operations;

- Based on the results, we defined and established such kind of structure, which could be the basement for organizing a complex CIS, that adequate for the NATO requirements and able to support the multinational cooperation. The planning system has to be defined on the operational claims, on the system requirements and on the opportunity of the technical realisation. This triple factor appears in all cases according to the continuous control and the basic principle of feedback in the workflow;

- From our experiences the present field communication system does not form an unifined system, and it is not fit for the modern operational challenges. That's why we suggest to use (buy) modern and complex field CIS which could support equally the command of traditional and the crisis operations.

6. SCIENTIFIC RESULTS

- By analyzing and evaluating of the thesis related documents (laws, norms, doctrines) we have determined the CIS abilities and requirements regarding to crisis response operations and we defined novel terms of it;

- Compared the experiences of international roles and the strategic-tactical abilities we defined the requirements of the crisis response operations supporting CIS. We defined those factors as well, which are influencing the organization and planning methodologies of CIS;

- We defined the unified and complex supporting demand CIS elements of traditional and crisis response operations related command and control.

7. RECOMMENDATIONS FOR PRACTICAL USAGE

In our opinion, the results of the thesis could be used in the organization of CIS elements in crisis response operations. These can be integrated into the educational system – both for BSc and MSc level and further professional training – of the Bolyai János Military Technical Faculty of the Zrínyi Miklós National Defence University.

The described and determined organizational principles could offer a very good basement for further research of the related topics and for other special fields (info security, informatics, technical tools, abilities offered by networks) analyzes and PhD works.

REFERENCES

[1] Rajnai Zoltán: A kommunikációs rendszerek tervezését segítő szoftverek igényei, In.: „Kommunikáció 2000” nemzetközi szakmai tudományos konferencia kiadványa, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2000; p.:147.
[2] 94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről, In.: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 120. szám; 1998. december 29.; p.: 8271
[3] Szenes Zoltán: 10 éves NATO tagság és a haderő átalakítása, In.: Honvédségi Szemle; 63. évf. 2. szám (2009. március); p.: 7. (HU ISSN 1216-7436)
[4] Eck Péter: Az MH ÖHP Híradó és Informatikai Főnökség, In.: Előadás a ZMNE Híradó Tanszék részére; Székesfehérvár, 2010. február 24.; dia:7.
[5] Tóth Barnabás: Magyar katonai szerepvállalás a balkáni béketámogató műveletekben, In.: Kard és Toll 2007/1. (2007); p.: 23. (ISSN: 1587-558X)
[6] Rajnai Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO-országok kommunikációs rendszereinek tükrében (doktori PhD értekezés) Budapest, 2001
[7] Resperger István: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során (doktori PhD értekezés) Budapest, 2001 p.:
[8] Kőszegvári Tibor: A válságkezelés aktuális problémái, In.: ZMKA Közlemények, 1994, 202. szám; p.217.
[9] Deák János: Napjaink és a jövő háborúja, In.: Hadtudomány a Magyar Hadtudományi Társaság folyóirata XV. évfolyam 1. szám (2005. március) (ISSN: 1215-4121)
[10] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás, Honvédelmi Minisztérium kiadványa, 2010; p.: 27-28.

[11] Rábai Zsolt: Viták az új stratégiai koncepció körül, In.: A NATO formálódó új stratégiai koncepciója és Magyarország; Konferencia előadás 2010. március 25.; ZMNE Budapest
[12] Bencze Balázs–Hegedüs Zoltán–Kolossa Sándor–Padányi József–Praveczki Zoltán–Szternák György: A Válságreagáló műveletek elmélete és gyakorlata a 21. században, Egyetemi jegyzet; ZMNE Budapest 2004; p.: 66.
[13] Szenes Zoltán: A NATO-transzformáció hatása Magyarországra, a Magyar Honvédségre, In.: http://www.hm.gov.hu/hirek/kiadvanyok/uj_honvedsesegi_szemle/a_natotranszformacio (letöltve: 2009.02.14.)
[14] Gácser Zoltán: Tűzszerész és felderítő robotok a magyar haderőben, In.:http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/gacser_rw7.html (letöltve: 2009.04.23.)
[15] Horváth József: A Magyar Honvédség képességfejlesztési tervei, figyelembe véve a NATO képességfejlesztési programjait és azok kereteit, Előadás, 2009. december 02.; Védelmi és Biztonsági Fórum (VBEF) harmadik ülése
[16] Szenes Zoltán: A NATO jövője Új stratégiai koncepcióra van szükség, In.:http://www.biztonsagpolitika.hu/userfiles/file/PDF/nato_jovoje.pdf (letöltve: 2009.12.10.)
[17] Sticz László – Csák Zoltán: Az expedíciós képesség és műveletek tartalmi elemeinek vizsgálata, In.: http://www.hm.gov.hu/files/9/9988/03.pdf (letöltve: 2008.10.18.)
[18] 51/2007. (VI. 6.) OGY határozat a Magyar Honvédség további fejlesztésének irányairól, In.: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 69. szám; 2007. június 6.; p.: 4901
[19] Szenes Zoltán: Politikai viták – lehetséges katonai következmények, In.: A NATO formálódó új stratégiai koncepciója és Magyarország; Konferencia előadás 2010. március 25.; ZMNE Budapest
[20] Dr. Szekeres Imre honvédelmi miniszter: Tájékoztató az Országgyűlés Honvédelmi és rendészeti bizottsága, valamint a Külügyi és határontúli magyarok bizottsága részére a Magyar Köztársaság Nemzeti Katonai Stratégiájáról, 2008. december, In.:http://www.hm.gov.hu/files/9/10970/tajekoztato_mk_nks.pdf (letöltve: 2009.06.21.)
[21] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás, Honvédelmi Minisztérium kiadványa, 2010; p.: 20.
[22] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás, Honvédelmi Minisztérium kiadványa, 2010; p.: 52.
[23] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás, Honvédelmi Minisztérium kiadványa, 2010; p.: 57-59.
[24] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében (doktori PhD értekezés) Budapest, 2007 p.: 6.
[25] Munk Sándor: KATONAI INFORMATIKA II.; Katonai informatikai rendszerek, alkalmazások; Egyetemi jegyzet; ZMNE Budapest, 2006; p.: 8.
[26] Haig Zsolt: Az információs műveletek, a sigint és az elektronikai hadviselés kapcsolatrendszere, In.: Felderítő Szemle, VI. évfolyam különszám; Budapest, 2007 február, p. 30.
[27] Kovács László: Gondolatok napjaink technológiájáról és a digitális hadszíntér kapcsolatáról, In.:http://www.zmne.hu/tanszekek/ehc/konferencia/april2001/kovacs.html (letöltve: 2009.06.21.)

[28] A Magyar Köztársaság Nemzeti Biztonsági Stratégiája, In.:http://www.kulugyminiszterium.hu/NR/rdonlyres/0AA54AD7-0954-4770-A092-F4C5A05CB54A/0/bizt_pol_hu.pdf (letöltve: 2009.05.25)
[29] Kovács Károly: Az EBESZ, a NATO és az Európai Unió békefenntartó tevékenységének alakulása a hidegháború után /diplomamunka/ ZMNE, Budapest 2008; p.: 42.
[30] Military Technical Agreement between the International Security Force ("KFOR") and the Governments of the Federal Republic of Yugoslavia and the Republic of Serbia, In: http://www.nato.int/kosovo/docu/a990609a.htm (letöltve: 2009.06.21.)
[31] A TANÁCS HATÁROZATA (2006. november 30.) Koszovó számára nyújtandó kivételes pénzügyi támogatásról (2006/880/EK) In.: Az Európai Unió Hivatalos Lapja L 339/36 (2006.12.06) http://epa.niif.hu/00800/00878/00895/pdf/00360038.pdf (letöltve: 2009.06.21.)
[32] 59/1998. (X. 15.) OGY határozat a Magyar Köztársaság hozzájárulásáról a koszovói válság megoldását célzó NATO-fellépéshez, In.: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 94. szám; 1998. október 15.; p.: 5888
[33] 54/1999. (VI. 16.) OGY határozat a koszovói békefenntartásban részt vevő nemzetközi erők (KFOR) tevékenységének elősegítéséről, In.: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 52. szám; 1999. június 16.; p.: 3358
[34] 55/1999. (VI. 16.) OGY határozat magyar kontingens részvételéről a koszovói békefenntartásban részt vevő nemzetközi erőkben (KFOR), In.: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 52. szám; 1999. június 16.; p.: 3359
[35] Tóth András: A béketámogató és békefenntartó műveletek híradása /diplomamunka/ ZMNE, Budapest 2004; p.: 28.
[36] Fekete Károly: VSAT rendszerek alkalmazásának lehetőségei a Magyar Honvédség jelenlegi és távlati hírrendszerében, In.: http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/KF_3.html (letöltve: 2009.06.21)
[37] Németh András: A mobil szolgáltatók hálózatainak felhasználása, fejlesztési lehetőségei és alternatív megoldások a katasztrófavédelmi kommunikáció területén (doktori PhD értekezés) Budapest, 2007 p.: 103.
[38] Hóka Miklós: A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO tagországok rádiórendszereinek vizsgálata tükrében (doktori PhD értekezés) Budapest, 2005 p.: 74.
[39] A honvédelmi miniszter 97/2008. (HK 13.) HM határozata a Magyar Honvédség Őr- és Biztosító Zászlóalj ideiglenes katonai szervezet megszüntetéséről, In.: Honvédelmi Közlöny a Honvédelmi Minisztérium Hivatalos Lapja, CXXXV évfolyam 13. szám (2008. augusztus 18.); p.: 999-1000.
[40] NATO Kosovo Force (KFOR) In.:http://www.nato.int/kfor/structur/nations/placemap/kfor_placemat.pdf (letöltve: 2010.02.26.)
[41] Koszovó CIMIC kézikönyve; A Magyar Honvédség Összhaderőnemi Parancsnokság kiadványa, 2009; p.:35.
[42] A Honvédelmi Minisztérium Honvéd Vezérkar főnökének 82/2008. (HK 7.) HM HVKF intézkedése a NATO KFOR Nyugati Többnemzetű Alkalmi Harci Kötelékben részt vevő katonai szervezet megalakításáról és felkészítéséről, In.: Honvédelmi Közlöny a Honvédelmi Minisztérium Hivatalos Lapja, CXXXV. Évfolyam 7. szám (2008. április 17.); p.:512.
[43] 41/2008. (HK 8.) HM JSZÁT- HM HVKF együttes intézkedés: A NATO KFOR Nyugati Többnemzetű Alkalmi Harci Kötelékben résztvevő Magyar Honvédség KFOR Zászlóalj híradásáról, informatikai támogatásáról és információvédelméről, In.: Honvédelmi Közlöny a Honvédelmi Minisztérium Hivatalos Lapja, CXXXV. Évfolyam 8. szám (2008. május 9.); p.:632.

[44] 1992. évi LXXII. törvény a távközlésről (A távközlésről szóló 1992. évi LXXII. törvény mellékletének 29. pontja) In.: http://www.1000ev.hu/index.php?a=3&param=8925 (letöltve: 2009.05.21.)
[45] Sándor Miklós–Magyarné Kucsera Erika: A zártcélú hálózat forgalmi optimalizálásának problémái, In.: Kard és Toll 2005/3; ZMNE; Budapest, p.: 107. (ISSN: 1587-558X)
[46] 1992. évi LXXII. törvény a távközlésről (A távközlésről szóló 1992. évi LXXII. törvény mellékletének 8. pontja) In.: http://www.1000ev.hu/index.php?a=3&param=8925 (letöltve: 2009.05.21.)
[47] Hóka Miklós: A Magyar Honvédség harcászati rádiórendszerének kialakítási lehetőségei egyes NATO tagországok rádiórendszereinek vizsgálata tükrében (doktori PhD értekezés) Budapest, 2005 p.: 70.
[48] Horváth Ferenc: A frekvenciagazdálkodás feladata és szerepe a Magyar Honvédségben, In.:http://www.hm.gov.hu/hirek/kiadvanyok/uj_honvedsesegi_szemle/a_frekvenciagazdalkodas (letöltve: 2009.01.11.)
[49] Globális háború közepén? In:http://www.demokrata.hu/heti-hir/globalis-haboru-kozepen?mini=programnaptar/2009/12/all& (2009.12.21.)
[50] Németh József: Irak Szaddam bukása után, In: Szakmai Szemle a Katonai Biztonsági Hivatal Tudományos Tanácsának Kiadványa 2007/1; p.: 63 (ISSN: 1785-1181)
[51] Magyar Honvédség Civil-katonai Együttműködési és Lélektani Műveleti Központ: Irak CIMIC kézikönyve Második, átdolgozott kiadás, Budapest 2006. február; p.. 43
[52] 54/2003. (V.6.) OGY határozat Irak demokratikus újjáépítéséhez szükséges stabilizációs és humanitárius feladatokban részt vevő nemzetközi erők tevékenységének elősegítéséről, In: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 46. szám; 2003. május 6.; p.: 4107
[53] 65/2003. (VI. 3.) OGY határozat az iraki válság rendezése érdekében tett erőfeszítésekhez történő magyar katonai hozzájárulásról, In: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 61. szám; 2003. június 03.; p.: 4978
[54] 119/2003. (XI. 5.) OGY határozat az iraki válság rendezése érdekében tett erőfeszítésekhez történő magyar katonai hozzájárulásról szóló 65/2003. (VI. 3.) OGY határozat módosításáról, In: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 126. szám; 2003. november 05.; p.: 9511
[55] http://wapedia.mobi/en/Multinational_Division_Central-South (letöltve: 2009.01.23.)
[56] http://www.hm.gov.hu/honvedseg/mhohp (2009.01.23.)
[57] Tóth András: A béketámogató és békefenntartó műveletek híradása /diplomamunka/ ZMNE, Budapest 2004; p.: 49.
[58] 1995. évi LXV. Törvény az államtitokról és a szolgálati titokról, In.:http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99500065.TV (2009.06.21.)
[59] Munk Sándor: Katonai Informatika II.; Katonai informatikai rendszerek, alkalmazások Egyetemi jegyzet; ZMNE, Bp. 2006
[60] Magyar Honvédség Civil-katonai Együttműködési és Lélektani Műveleti Központ: Irak CIMIC kézikönyve Második, átdolgozott kiadás, Budapest 2006. február; p.. 44.
[61] Csermely Nóra: Petersberg, In: http://www.grotius.hu/publ/displ.asp?id=XWRNWH (letöltve: 2009.02.22.)
[62] 62/2001. (IX. 25.) OGY határozat a Magyar Köztársaságnak az Amerikai Egyesült Államokat ért terrortámadást követő kül- és biztonságpolitikai lépéseiről, In: Magyar Közlöny a Magyar Köztársaság hivatalos lapja; 104. szám; 2001. szeptember 25.; p.: 7045
[63] 78/2006. (HK 16.) HM utasítása az afganisztáni tartományi újjáépítési csoportban résztvevő katonai szervezet létrehozásának feladatairól, valamint a személyi állomány kihelyezésének előkészítéséről és végrehajtásáról, In.: Honvédelmi Közlöny a

Honvédelmi Minisztérium Hivatalos Lapja, CXXXIII. Évfolyam 16. szám; 2006. augusztus 10.; p.:1111.
[64] http://www.hm.gov.hu/honvedseg/mh_tartomanyi_ujjaepitesi_csoport (letöltve: 2009.01.11.)
[65] http://www.nato.int/isaf/docu/epub/pdf/placemat.pdf (letöltve: 2009.05.25.)
[66] http://www.isaf.nato.int/en/troop-contributing-nations/index.php (letöltve: 2009.05.25.)
[67] Takács Judit, Landesz Tamás, Tálas Péter: A tartomány újjáépítési csoportokról, In.: ZMNE Stratégiai Védelmi Kutatóközpont elemzések – 2006/3; p.: 12.
[68] ISAF misszió; Háttéranyag, In.:http://www.hm.gov.hu/files/9/10252/hatteranyag-prt_2008_06_10.pdf (2009.05.25.)
[69] MH Tartományi Újjáépítési Csoport (MH PRT) In.:http://www.hm.gov.hu/honvedseg/mh_tartomanyi_ujjaepitesi_csoport (letöltve: 2009.01.11.)
[70] Munk Sándor: KATONAI INFORMATIKA II.; Katonai informatikai rendszerek, alkalmazások; Egyetemi jegyzet; ZMNE Budapest, 2006; p.: 179.
[71] STU II., In.: http://en.wikipedia.org/wiki/STU-II (2009.05.25.)
[72] ELSŐDLEGES FELADAT A MŰVELETEK TÁMOGATÁSA Beszélgetés dr. Lehel György dandártábornokkal, a NATO Híradó és Informatikai Rendszerek Szolgáltatásait Biztosító Ügynökség (NCSA) műveleti igazgatójával, In: Honvédségi Szemle; 63. évf. 5. szám (2009. szeptember); p.: 78. (letöltve: 2009.12.10.)
[73] Thales to Provide ISAF with Secure Voice and Data Services, In: http://www.deagel.com/news/Thales-to-Provide-ISAF-with-Secure-Voiceand-Data-Services_n000001132.aspx (letöltve: 2009.05.25.)
[74] THALES WILL DELIVER COMMUNICATION SERVICES TO NATO IN AFGHANISTAN, In.:http://www.thalesgroup.com/Press_Releases/Thales_will_deliver_communication_services_to_NATO/ (letöltve: 2009.05.25.)
[75] FOCUS ON FOC+ SERVICE CONTRACT FOR ISAF, In.:http://www.thalesgroup.com/News_and_events/LandJoint_Focus_20080624_ISAF/ (letöltve: 2009.05.25.)
[76] Rajnai Zoltán – Takács Péter: Az afganisztáni missziós híradás tapasztalatai, In.: Kard és Toll 2006/3; ZMNE; Budapest, p.: 31 (ISSN 1587-558X)
[77] A Honvédelmi Minisztérium Honvéd Vezérkar főnökének 125/2008 (HK 13.) HM HVKF intézkedése az afganisztáni műveleti területen belüli használatra az amerikai hadseregtől kapott HMMWV páncélozott terepjáró gépjárművek átvételével és üzemben tartásával kapcsolatos feladatokról, In.: Honvédelmi Közlöny a Honvédelmi Minisztérium Hivatalos Lapja, CXXXV. Évfolyam 13. szám; 2008. augusztus 18.; p.:1024-1026.
[78] Bocskai István, a Honvédelmi Minisztérium szóvivője: RPG-s támadás érte a magyarokat Afganisztánban, In.:http://www.honvedelem.hu/cikk/24/18274/rpg-s_tamadas_afganisztan.html (letöltve: 2010. 02. 15.)
[79] Mező András: A rögtönzött robbanószerkezetek elhárításáról, In: Honvédségi Szemle; 63. évf. 1. szám (2009. január); p.: 20.
[80] Makk László-Hajdú László: Az improvizált robbanóeszközök alkalmazásáról, In.: Új Honvédségi Szemle LXI. évfolyam 3. szám (2007. március); p.: 5-21. (ISSN 1216-7436)
[81] Hóka Miklós: A csúcstechnológia alkalmazása a hadszíntéren a szoftverrádiótól a nanotechnológiáig, In.: Szakmai szemle; A Katonai Biztonsági Hivatal Tudományos Tanácsának kiadványa; Budapest, 2006/2. szám; p.:76-77. (ISSN: 1785-1181)

[82] Comtech Telecommunications Corp. Receives $2.5 Million Purchase Order Amendment for NATO Force Tracking System, In.: http://comtechmobile.com/pr020607.html (letöltve: 2009.05.25.)
[83] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás Honvédelmi Minisztérium kiadványa, 2010; p.: 68.
[84] Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében (doktori PhD értekezés) Budapest, 2007 p.: 108.
[85] Magyar Sándor: Katonai kommunikációs igények lehetőségek a békefenntartás vezetésének támogatásában (doktori PhD értekezés) Budapest, 2008 p.: 21.
[86] Magyar Sándor: Katonai kommunikációs igények lehetőségek a békefenntartás vezetésének támogatásában (doktori PhD értekezés) Budapest, 2008 p.: 23.
[87] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás Honvédelmi Minisztérium kiadványa, 2010; p.: 23.
[88] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás Honvédelmi Minisztérium kiadványa, 2010; p.: 82.
[89] Ványa László: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységekre (doktori PhD értekezés) Budapest, 2001
[90] Koronczai Tibor: Missziós híradó-felkészítés az MH 43. Nagysándor József Híradó és Vezetéstámogató Ezrednél, In: Honvédségi Szemle; 64. évf. 1. szám (2010. január); p.: 16. (HU ISSN 2060-1506)
[91] Magyar Sándor: Katonai kommunikációs igények lehetőségek a békefenntartás vezetésének támogatásában (doktori PhD értekezés) Budapest, 2008 p.: 26.
[92] http://www.hm.gov.hu/miniszterium/mh_muvelet_iranyito_kozpont (letöltve: 2009.05.25)
[93] Süle Attila–Csabianszki Viktor: A Magyar Honvédség tapasztalatfeldolgozó rendszeréről, In: Honvédségi Szemle; 62. évf. 1. szám (2008. július); p.: 16. (HU ISSN 2060-1506)
[94] A NATO szárazföldi csapatok híradó és informatikai rendszerei kapcsolatának minimális mértéke (STANAG 5048); A Honvédelmi Minisztérium Honvéd Vezérkar Katonai Tervező Főcsoportfőnökség Kiadványa; 2006 (Nyt. szám: 69-27/NATO)
[95] Sándor Miklós–Farkas Tibor–Jobbágy Szabolcs: Híradásszervezés jegyzet a BJKMK híradó tanszék BSc, MSc, és PhD hallgatói számára; ZMNE Budapest, 2009; p.: 13-14.
[96] Bene Iván: A Magyar Honvédség tábori híradásának fejlesztése, a fejlesztés 2004. évi időszerű kérdései – 6. dia; MH HVK Híradó és informatikai Csoportfőnökség Elvi Tervező Osztály; Budapest, 2004.
[97] Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben II. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 122-137. oldal)
[98] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal)
[99] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal)

Kendernay Zsolt – Takács Attila – Pándi Erik – Dorkó Zsolt
kendernayz@mail.ahiv.hu – attila.takacs@mail.ahiv.hu – pandi.erik@zmne.hu – dorkozs@emgei.police.hu

A KÉSZENLÉTI SZERVEK TEVÉKENYSÉGÉT TÁMOGATÓ KÖZÖS INFRASTRUKTÚRA[1]

Absztrakt

Jelen közlemény bemutatja a készenléti szervek támogatására kialakítható IT rendszer alapjait.

This publication introduces the foundations of an IT system which could be set up to support emergency services.

Kulcsszavak: *IT rendszer, katasztrófavédelem, mentők, rendőrég ~ IT network, disaster management, ambulances, police*

BEVEZETÉS

A készenléti szervezetek szükségesnek tartják, hogy feladatuk ellátásához egymással kapcsolatot teremtsenek. Ennek technikai, műszaki, informatikai feltétele egyelőre még nem teljesen azonos, azonban a tervezett fejlesztésekkel jó részük megoldhatóvá válik. Ahhoz, hogy az új lehetőségeket megfelelő módon használják több, és különböző szintű egyeztetésekre van szükség. Ezek az egyeztetések elkezdődtek az Országos Rendőr-főkapitányság (ORFK), az Országos Katasztrófavédelmi Főigazgatóság (OKF) és az Országos Mentőszolgálat (OMSZ) között mind felsővezetői, mind alsóbb szinteken, többek között az informatikai szakemberek között is. Jelen közleményben az infokommunikációs együttműködési lehetőségekre kínálunk megoldást, amely elsődlegesen az adatátviteltechnikai és távközlési területeket érinti.

1. AZ EGYSÉGESÍTÉS OKA

A készenléti szervezetek együttműködésnek szükségessége nem vitatható, ugyanakkor megemlítjük, hogy magával a meglévő készenléti szervezetekkel és szervezeti tagozódásával kapcsolatban már nem ennyire egyértelmű a válasz és ezzel kapcsolatban különböző vélemények látnak napvilágot. Jelen kérdéskört közleményünk azonban nem vizsgálja, hanem a meglévő készenléti szervezetek infokommunikációs együttműködésére keresi a választ.

Mielőtt azonban a konkrét megvalósítási lehetőségeket áttekintenénk, nézzük meg miért, milyen területen és formában szükséges az egységesítés.

A készenléti szervezetek feladatuk ellátása során kooperálnak egymással szervezeti, operatív, és technológiai, műszaki szinten. Vagyis, ha példa okán egy baleset miatt értesítik a rendőrséget, és a helyszínen kiderül, hogy van sérült, akkor természetesen hívják a mentőket, és szükség esetén a tűzoltókat is. Mindehhez mobilkészüléket használnak, vagy ma már egyre több helyen az EDR-n keresztül veszik fel a kapcsolatot. De ezen kívül más nem történik. Tehát a már rögzített adatokat, nem tudják egymáshoz eljuttatni, azt mindegyik

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

szerv külön-külön adminisztrálja, miközben a mai technológia erre már alkalmas. Ez olyan mértékű idő, pénz és információ veszteség, ami egy egységes Infokummunikációs kapcsolattal megoldható.

Ha a témával kapcsolatban egységesítést hallunk, akkor különböző szintekre gondolunk, melyet célszerű hármas tagozódásra bontani. Az egyik egységesítési szint strukturális, vagyis egy-egy szervezet, intézmény közös platformara hozása, (tűzoltóság, katasztrófavédelem), vagy egy szervezeten belüli átalakítás például, amikor osztályokat vonnak össze. A másik szint operatív jellegű, amikor a tevékenységek koordinálását centralizálják. A harmadik szint műszaki, technológiai, ami az eszközök alkalmazását centralizálja, a negyedig szint az informatikai, vagy más néven infokommunikációs szint, ahol különböző formában és módon kínálkozik lehetőség az egységesítésre.

Az egységesítés megvalósítható az OSI modell fizikai, adatkapcsolati, hálózati és szállítási szintjén, melyet együtt hálózati szintként aposztrofálunk és a viszonylati, megjelenítési és alkalmazási réteg szintjén, melyet alkalmazási szintnek nevezünk.

Az egységesítés megvalósításának lehetőségét hálózati infrastrukturális szinten mutatjuk be, melynek eredménye előnyöket és hátrányokat egyaránt magában foglal.

2. AZ EGYSÉGESÍTÉS HÁTRÁNYA ÉS ELŐNYEI

Az egységesítés előnyeit és hátrányait vizsgálva megállapítható, hogy sokkal több szól mellette, mint ellene. Hátránya leginkább abban jelentkezhet, hogy a hálózati infrastruktúra nem valamelyik készenléti szervezet tulajdona és az üzemeltetés sem saját felügyelet alá tartozik. Az sem állítható, hogy a 112-es alapú Egységes Segélyhívó Rendszer (ESR) egységes infrastruktúra nélkül nem kivitelezhető. Mégis, ha hatékonyságra és gazdaságosságra törekszünk célszerű az egységes infrastruktúra kialakítását választani, hiszen számtalan előnye sorolható fel. A már most is meglévő országos lefedettségen és a megyei, régiónkénti központokon felül, a létrejövő egységes gerinchálózati infrastruktúra egy zárt, redundáns hálózat, melyen keresztül dedikált sávszélességhez, integrált beszéd és adatátvitelhez, megfelelő adatbiztonsághoz juthatnak a szervezetek. Ezen felül meghatározható a forgalmi prioritások, a zökkenőmentes input-output adattovábbítás, a rugalmas 24 órás hibakezelés. A biztonságos gyors kommunikáció révén pontosan az érhető el, ami a katasztrófahelyzetekben elengedhetetlen: egy mindentől független, önálló, minőségi szolgáltatást nyújtó átviteltechnikai hálózat, mely egységesen magas színvonalon biztosítja a készenléti szervezetek közötti kommunikációt. A gazdaságos üzemeltetés, a tapasztalt szakemberek mind-mind lehetővé teszik, hogy európai szintű segélynyújtási szolgáltatást kapjanak az igénybevevők. Mindezek mellett nem elhanyagolható, hogy létrejön az egységes készenléti rendszer alapja, mely a hálózat egységességét az alrendszerek azonos strukturális, technológiai és eszközrendszeri felépítését, valamint a részek azonos szolgáltatás-hozzáférési, rendszer-felügyeleti és üzemviteli szervezését biztosítja.

Egyébiránt, mint látható az egységesítésnek sok az előnye, hiszen a megnövekedett sávszélesség gyorsabb, hatékonyabb szolgálat-, bevetés-, mentésirányítást tesz lehetővé. Ezáltal rövidebb idő alatt adható segítség és jobban kivédhető az esetleges nagyobb káresemény bekövetkezése is. Az emberéletek viszonylatában is jelentős változás következik be, hiszen a gyors és hatékony vészhelyzetek megoldása nagymértékben növeli az emberélethez és testi épséghez való alkotmányos jogokat.

3. A SZOLGÁLAT, BEVETÉS ÉS MENTÉSIRÁNYÍTÁSI RENDSZEREK FUNKCIÓI, SZOLGÁLTATÁSAI ÉS KÖVETELMÉNYEI

A készenléti szervezetek a 112-es nemzetközi segélyhívószám kapcsán, tervezetten egy európai színvonalú segélyhívás szolgáltatást hoznak létre. Az Európai Bizottság alapfeladatnak tartja a segélyhívó fél azonosítására, illetve a helymeghatározására vonatkozó

adatok rendelkezésre állását. Az egységes segélyhívás kezelése, és a segélyszolgálattal kapcsolatos feladatok hatékony, a kor igényeinek megfelelő támogatása érdekében az ORFK, az OKF és az OMSZ operatív feladatirányító rendszerek megvalósítását szándékszik végrehajtani. Látható, hogy a készenléti szervezetek saját hatáskörben, saját feladataik támogatását segítő, egymástól elkülönülő független rendszer létrehozását tervezik, amelyek csak hálózatba kötve alkalmasak az Európai Unió által támasztott követelmények megfelelésére, és az egységes segélyhívás megteremtésére.

Ennek kialakításához a készenléti szervezeteknek szükségük van arra, hogy az általuk fejlesztett rendszerek korszerű kommunikációs infrastruktúrán álljanak összeköttetésben, és köztük a fizikai szintű adatcsere biztosított legyen. Az országos szintű kommunikációs infrastruktúra zavartalan működését az EKG és a KEK KH zRH-ja együttesen képes biztosítani. Fontos újra kiemelni, hogy a rendszerek alkalmazás szintű kommunikációjáért, logikai kapcsolatának kialakításáért az egyes készenléti szervezetek felelnek, a zRH csak a fizikai adatkapcsolatot biztosítja.

4. AZ ELŐSZŰRÉS ÉS AZ EDR

A tervezett segélyhívó rendszer működésének lényegi eleme, hogy a segélyhívások előfeldolgozása az ORFK-nél történik majd, de a végrehajtás továbbra is az önálló szakmai felelősséget hordozó készenléti szervezetek feladata marad. A segélyhívásokat fogadó, a hívó fél kikérdezése alapján eldönti, hogy a hívás valóban segélyhívás-e, és ha igen, akkor az melyik készenléti szervezet hatáskörébe tartozik, majd az adatokat ennek megfelelően továbbítja.

A híváselosztás a területi illetékességnek megfelelően automatikusan történik és nem a kikérdezést követően, hanem már azt megelőzően. A 112-es hívásfogadón keresztül a rendőrség, a tűzoltók és a mentők irányító központjai közel azonos időben juthatnak a hatékony intézkedést lehetővé tevő információhoz. Ezt követően a segítség természetének megfelelően intézkednek saját szakmai előírásaik és tevékenységük felelősségi szabályai szerint. Az érintett készenléti szervezetek a többirányú segélynyújtást igénylő események során tevékenységük egymás közötti koordinálására az EDR-t is használják.

A kiépített és országos lefedettséget biztosító digitális EDR a készenléti szervezetek rádiókommunikációját biztosítja, vagyis az EDR a készenléti szervezetek bevetés-irányítási rendszerének rádiókommunikációs háttere. A készenléti szervezetek elkülönülő szakmai tevékenységéből adódóan az EDR-en belül virtuális magánhálózatok - VPN - kerültek definiálásra, amelyek biztosítják az egyes felhasználói szervezetek zavartalan rádióforgalmazását és megakadályozzák az illetéktelen hozzáférést. A szervezeteken belüli rádiókommunikációs jogosultságokat a VPN gazdaszervezetek kezelik és ellátják a VPN-en belüli forgalomszervezést. A készenléti szervezetek elkülönülő szakmai tevékenysége az EDR-en belüli csoportképzésekkel és jogosultságokkal teljes mértékben biztosítható.

A tevékenységirányító ügyeleteken asztali rádióterminál, diszpécser és automatikus helymeghatározási, úgynevezett AVL munkaállomások kerültek már letelepítésre. A tevékenységirányítás a definiált forgalmi csoportokon történik, a szervezeten belüli együttműködéseket az illetékes ügyelet tudja szervezni és biztosítani. A felhasználó szervezeteknek az EDR-en belül lehetőségük van a tevékenységirányításhoz hang- és adatkommunikációt használni. A tevékenységirányítás során esetlegesen fellépő speciális igényeket és az elkülönülő – megyei rendőr-főkapitányságok, katasztrófavédelmi ügyeletek, mentők közötti együttműködést a megfelelő csoportképzésekkel a KEK KH – mint központi VPN menedzser szervezet végzi. A tevékenység irányítás során a kárhelyszíni együttműködésre az egyes felhasználók között nyílt, operatív együttműködési csoportok állnak rendelkezésre. Így nemcsak a közvetlen irányító ügyeletükkel tudnak kommunikálni, hanem adott esetben, a mentésben résztvevő más szervezet tagjaival is. Ugyanakkor a

kárhelyszíni együttműködés során használt rádióforgalmazást a bevetés-irányítási ügyeleteken is hallják, így biztosított a megfelelő információáramlás.

5. HÁLÓZATI KATASZTRÓFATŰRŐ KÉPESSÉG

A zRH jelenleg is tartalmaz önmagában redundáns útvonalakat a hibatűrő képesség és a rendelkezésre állás megfelelő szintű biztosítása érdekében. Nem csak a készenléti szervezetek, hanem a zRH is komoly fejlesztések elé néz, mely a sávszélesség bővülésén túl a katasztrófatűrő képesség növekedésével is jár. Ez szakmailag, európai viszonylatban is kimagasló eredményt jelenthet, hiszen a két országos, technológiában, és adatkapcsolati utakban jelentősen eltérő hálózat - az EKG és a zRH, mint EKG alhálózat – összekapcsolásra kerül. Ugyan a két hálózat jelentősen eltérő kommunikációs útvonalakat, de kompatibilis kommunikációs technológiát használ, a redundáns útvonalak növelése és ezzel a katasztrófatűrő képesség jelentős mértékben megemelkedik, mely indokolt is a hálózatokra csatlakozó, kiemelt feladatokat ellátó készenléti szervezetek számára. Meg kell említeni, hogy a már meglévő és a kibővült hálózat más kormányzati és közigazgatási szervnek is nyújt szolgáltatást, melyet a 22-es ábra - a teljesség igénye nélkül - szemléltet.

6. A KÖVETELMÉNYRENDSZEREK SPECIFIKÁCIÓJA

Mint ismeretes a szervezetek mindegyike saját hatáskörben lévő, különálló szolgálat-, bevetés- és mentésirányítási rendszert kíván kialakítani. Annak érdekében, hogy ezek a struktúrák egységes készenléti rendszerként, országos szinten tudják kezelni a legtöbbször szerveken és rendszereken átívelő segélyszolgálati folyamataikat elengedhetetlenül szükséges a fizikai adatkapcsolatot biztosító hálózati infrastruktúra, melyet a KEK KH a zRH-n keresztül tud biztosítani a készenléti szervezetek számára. A szervezetek az említett rendszerrel támasztott igényeit a következőkben külön – külön mutatjuk be.

6.1. Országos Rendőr-főkapitányság

Az ORFK a Rendőrség 112-es segélyhívó, ügyeleti és szolgálatirányítási rendszerének komplex, országos fejlesztését kívánja megvalósítani, melynek révén létrejön egyfelől a Rendőrség által jelenleg üzemeltetett, a 112-es hívószámon valamennyi távközlési hálózatból elérhető segélyhívó rendszer fejlesztése, illetve kialakításra kerül egy országos, a Rendőrség közreműködését igénylő események kezelését, megoldását hatékonyan segítő, elektronikus szolgálatirányítási rendszer.

A rendszer kialakításához felmerült igények

- valamennyi kommunikációs csatornán érkezett információ fogadása;
  - vokális hívások, rövid szöveges és multimédiás üzenetek (SMS és MMS), fax, e-mail, multimédiás (szöveg-, kép-, és hangállományt tartalmazó) tartalmak;
  - e-call hívások;
  - a meghatározott célcsoporto(ka)t kiszolgáló, telepített segélyhívó- és riasztóberendezések jeleinek, hívásainak fogadása, küldése;
  - internetes felület, és kommunikációs infrastruktúra.
- a hívó, illetve az információküldő fél, azaz az ügyfél azonosítása;
- a híváskezdeményező helyzetének meghatározása, és
- digitális térképen való megjelenítése;
- az esemény-lapok elektronikus továbbítása a kialakítandó szolgálatirányítási központokba;

- a 112-es európai segélyhívószám filozófiájának megfelelő, általános segélykéréssel kapcsolatos, elvárt minőségű tájékoztatás- és szolgáltatásnyújtása;
- valós időben, megfelelő térinformatikai támogatás mellett a rendelkezésre álló erők és eszközök helyzetének, státuszának követése.
- Összességében elmondható, hogy az ORFK olyan rendszer kialakítását szorgalmazza, amely elektronikus kapcsolat révén a szolgálatirányítási központok és az ügyeletek közötti hatékony információáramlást biztosítja, fogadja és nyugtázza az elektronikus úton érkező információkat (adatokat, kéréseket, riasztásokat, bejelentéseket stb.), valamint egységes elektronikus felületen (esemény-adatlap) regisztrálhatóvá tenni a kapitányságí hívószámokra érkező, illetve a személyesen tett bejelentéseket, amelyeket továbbítanak a területileg illetékes szolgálatirányítási központba.
- Ezen követelményeknek egy országos lefedettséggel rendelkező, korszerű adat és távközlési hálózat nyújt megfelelő hátteret.

6.2. Országos Katasztrófavédelmi Főigazgatóság

Az OKF célja elsősorban egy olyan Katasztrófavédelmi Operatív Tevékenységirányító Rendszer (KOTIR) kialakítása, amely a katasztrófavédelmi erők egységes feladatellátását úgy képes megvalósítani, hogy a katasztrófavédelemben résztvevő szervezetek információáramlása gyors, az IT kapacitások kihasználása hatékony legyen.

A KOTIR IT megvalósításához szükséges elvárások a következőkben foglalhatóak össze

- Vészhelyzetben biztosítani a szükséges információáramlást;
- Megteremteni a terepi viszonyok közötti adatkommunikációt;
- A bevetésre induló vészhelyzet-kezelést ellátó erők gyors és megbízható információellátása mobil adatkommunikációs eszközökkel, melyekkel elhelyezkedésüktől függetlenül képesek adat és információcserére;
- Lehetőséget adni a lakosság tájékoztatására;
- A mobilkommunikáció nyújtotta lehetőségek kihasználása riasztás, tájékoztatás, adatmenedzsment területén;
- Helymeghatározó képességek kiépítése;
- Lakossági kapcsolódási pontok megteremtése;
- Közös informatikai platform kialakítása a katasztrófakezelésben résztvevő szervezetekkel, mely egységes informatikai hátteret nyújt.

A fentieket összefoglalva elmondható, hogy az OKF egy olyan korszerű informatikai rendszerre tart igényt, amely gyors, megbízható költséghatékony és minden körülmények között képes (vészhelyzetben is) feladatai teljes körű támogatására. Mindehhez olyan hálózati infrastruktúrára van szükség, amely ezen elvárásoknak eleget tud tenni.

6.3. Országos Mentőszolgálat

Az OMSZ olyan mentésirányítási rendszert kíván létrehozni, mely kihasználja a digitális hálózatok összes előnyét.

A hálózattal szemben a következő elvárások fogalmazódtak meg:

- Az évente beérkező kb. 3,5 millió hívás gyors és szakszerű fogadása;
- az ország összes mentési alközpontjának a mai kornak megfelelő informatikai és távközlési eszközökkel történő felszerelése;

- a 21 alközpont digitális kommunikációjának redundáns kialakítása;
- az éves szinten 2,5 millió eset hatékony és gazdaságos kezelése;
- Mindezen feladatok elvégzéséhez olyan hálózati kapacitásra van szükség, amely ezen elvárásokat biztosítani tudja.

7. A HÁLÓZATI INFRASTRUKTÚRA MEGVALÓSÍTÁSA

A zRH szolgáltatásait igénybevevők, valamint a fent vázolt rendszerigények, olyan fizikai adatkapcsolatot feltételeznek, amelyekhez megfelelő szintű hálózati háttér szükséges. Ennek kivitelezését a következő pontban mutatjuk be.

8. TERVEZÉSI MEGFONTOLÁSOK

A megvalósításnál a következő szempontokat vettük figyelembe:

- Költséghatékony megvalósítás – elsődleges szempont a hosszú távú üzemeltetés költségeinek minimalizálása;
- A gerinchálózaton jelenleg biztosított valamennyi szolgáltatásnak a későbbiek során is működőképesnek kell lennie;
- A meglévő menedzsment központból a gerinchálózat, és a hozzá kapcsolódó szervezetek hálózati eszközeinek teljes mértékben menedzselhetőeknek kell lenni;
- A gerinchálózat aktív eszközei nagykapacitású kapcsolatokkal csatlakozzanak egymáshoz. A kapcsolatok kialakítása során a párhuzamos útvonalak között törekedni kell a terhelés megosztásra;
- A gerinchálózatnak alkalmasnak kell lenni integrált hang-adat átvitelre. Az ehhez szükséges Quality of Service (QoS) funkciókat biztosítani kell;
- A titkosított adatátvitel, preferáltan IPSec technológiával valósuljon meg. Az IPSec csatornákat a VPN központokban kell végződtetni.

9. A MEGVALÓSÍTÁS LÉPÉSEI

- A zRH-ra hosszútávon támaszkodó szervezetek, és az általuk használt informatikai rendszerek felhasználóinak és üzemeltetőinek infrastrukturális hálózati igényeihez a következőket kell elvégezni:
- Nagysebességű, megbízható távközlési adatkapcsolatok bővítése Budapest területén szervezetenként minimálisan 100Mbps csatlakoztatási lehetőséggel;
- Nagysebességű, megbízható távközlési adatkapcsolatok fejlesztése régiós illetve megye viszonylatokban, szervezetenként minimálisan 2-50Mbps csatlakoztatási lehetőséggel;
- Az szervezetek nagytávolságú hálózati infrastruktúrájában magas rendelkezésre állás megvalósítása, szükséges tartalékolások beiktatása, redundancia megteremtése;
- Digitális telefonhálózatok, telekommunikációs rendszerek átjárhatósága, összekapcsolása, egységes IP protokoll alapú tartalék útvonal és hívás irányítás lehetőségének kiépítése;
- Szervezetek közötti közös informatikai szolgáltatások lehetőségének megteremtése;
- Mobil-internetes és internetes felhasználók biztonságos kiszolgálása preferált IPSec VPN központ és szigorú authentikációs eljárások;
- Egységes hálózatmenedzsment és HelpDesk szolgáltatás, valamint üzemeltetési háttér;
- Egységes hívásfogadó diszpécser állomások kialakítása, hívás információk rögzítése;

- EDR kapcsolódási pontok kialakítása, központi VPN együttműködés kialakítása.

10. HÁLÓZATI INFRASTRUKTÚRA ELEMEI

A korábbiakból is látható a zRH hálózata már most is rendelkezik a felsoroltak nagy részével, ezért nem gondoljuk, hogy egy új hálózat kiépítésére van szükség, hanem elegendő a meglévő hálózati infrastruktúra bővítése, korszerűsítése, amely egyaránt megfelel a jövőbeni elvárásoknak és a készenléti szervezetek által támasztott követelményeknek. Megvalósításához az alábbi műszaki fejlesztéseket célszerű elvégezni:

- Országos mikrohullámú és budapesti optikai gerinchálózat;
  - A mikrohullámú gerinchálózat a Hármashatár-hegy, Galyatető, Misinatető, Kab-hegy és Kiskunfélegyháza között különböző sebességű mikrohullámú összeköttetések üzemelnek, melyek egységesítése szükséges;
  - A sávszélesség a felhordó hálózat bővítésével kiszolgálja, az OKF és az OMSZ igényeit.

- Megyei felhordó hálózatok bővítése, korszerűsítése;
  - készenléti szervezetek megyei irányító központjai, valamint az MRFK-k közti összeköttetés létesítése során ki kell építeni a kapcsolódást a Megyei Katasztrófavédelmi Igazgatóságok (MKI) és az Országos Mentőszolgálat (OMSZ) megyei szervezeteinek irányába.

- Országos MPLS hálózat és budapesti Gigabites hálózat;
  - A megnövekvő mikrohullámú gerinc és felhordó hálózati infrastruktúrára nagyobb kapacitású kapcsoló eszközöket, útválasztókat kell telepíteni, melyek kiszolgálják, a szervezetek adatkapcsolati igényeit mind gerinchálózati, mind végponti eszközök tekintetében.

- A hálózaton megvalósuló TDM over IP rendszer bővítése;
  - A még régebbi technológiák alkalmazása miatt emulációval kell biztosítani az E1-es transzparens átviteli utakat.

- Digitális távbeszélő hálózat és IP alapú távbeszélő szolgáltatás bővítése;
  - A hálózat digitális alközpontjainak fejlesztése, integrálása az IP technológiával. Ezzel lehetővé válik a társhálózatokkal való többrétű együttműködés, az EDR hálózathoz történő egyszerű átjárás, ami új lehetőségeket teremt a 112-es segélykérő hívások követelményeinek megfelelő kezelésére. A segélyhívást közvetítő hálózat feladata, hogy a segélyszolgálati állomások által fogadott segélyhívást,- ha további intézkedések szükségesek – a megfelelő szolgálat szakmai tevékenység irányító ügyeleteihez továbbítsa. Ez IP protokoll alapú hívásirányítással megvalósítható, melyet már néhány kapcsolódó szervezet jelenleg is használ, de a rendszer bővítésével ez kiterjeszthető lenne valamennyi szervezet irányába.

- 112-es hívások fogadása, információk rögzítése;
  - Ki kell alakítani a 112-es hívások, valamint az ezekhez kapcsolódó helymeghatározási információk fogadására, illetve az illetékes készenléti szervezethez történő eljuttatására alkalmas rendszert. Egy adott

segélyhívással kapcsolatos valamennyi információt egységesen, visszakereshető módon, eseményre rendezetten kell kezelni, melyhez a járulékos információkat naplózni és rögzíteni kell.

- Menedzsment rendszer kialakítása;
  - Ki kell alakítani egy olyan menedzsment rendszert, mely lehetővé teszi valamennyi eszköz és szolgáltatás felügyeletét. Ezáltal a rendszerekben jelentkező hibák felismerhetők, és a hibajelentések továbbíthatók a helyi szakemberek számára.

- Adatközpont (backup) központ kialakítása;
  - A zRH infrastruktúrája, az alkalmazott technológiák lehetőséget biztosítanak a készenléti szervezetek számára, hogy közösen alkalmazott szolgáltatásokat is igénybe vegyenek. Ilyen közös szolgáltatás lehet egy egységes levelező rendszer, vagy egy IP alapú hívásirányító rendszer, egy központi backup adattár vagy VPN központ. A közös szolgáltatásokat megvalósító központi erőforrások elhelyezésére szükséges egy védett adatközpont kialakítása. Az adatközpontban a központi erőforrások számára megteremthetők a biztonságos működési feltételek, illetve megbízható, nagysebességű redundáns hálózati kapcsolat biztosítható a szolgáltatói hálózatok irányába is. A közös szolgáltatások megvalósításának előnye, hogy nem kell szervezetenként kiépíteni és üzemeltetni, ezáltal költséghatékonyabb.

- EDR kapcsolódási pontok;

  Az EDR-hez történő illeszkedéshez, az alábbi fejlesztéseket szükséges megvalósítani:
  - AVL vonatkozásban: Szükséges a közcélú vezetékes és vezeték nélküli távközlési szolgáltatóktól érkező helymeghatározási adatokat fogadó és azt az illetékes szervezethez továbbító hálózati elem rendszerbe állítása, melynek feladata az EDR rendszerből érkező rádióterminálok GPS adatainak fogadása is, majd a rendőrség, katasztrófavédelem, mentők részére történő szelektálása, valamint továbbküldése a szolgálat-, bevetés- és mentésirányítási rendszerek felé;
  - SDS vonatkozásban: Az EDR rendszer alapszolgáltatásai közé tartozik a szöveges üzenetek küldése és fogadása. A készenléti szervezetek részéről érkezett és szolgálati igényként merül fel, hogy az arra jogosított rádióterminálokról közvetlenül - megfelelő authentikációt és naplózást követően - hozzáférjenek on-line adatbázisokhoz. Az adatbázishoz történő hozzáférés feltétele az SDS Gateway alrendszer üzembeállítása. Ezen keresztül ellenőrzött körülmények között biztosítható a folyamatos hozzáférés, ezzel is meggyorsítva a terepen dolgozó készenléti szervezetek munkáját.
  - A fentieken kívül még a következő elemek fejlesztését is célszerű végrehajtani:

- VPN központ és authentikációs megoldások bővítése;
- Help-Desk és felügyeleti rendszerek korszerűsítése;
- Hálózat rendelkezésre állásának növelése, tartalékolások kialakítása, redundáns eszközök alkalmazása;
- Hálózatbiztonsági kockázatok csökkentése, kizárása.

11. AZ EGYSÉGES INFRASTRUKTÚRA ÁBRÁZOLÁSA

A készenléti szervezetek jelenlegi helyzetének, várható fejlesztéseiknek, követelményrendszerüknek megfelelően a zRH hálózatát is bővíteni, korszerűsíteni kell, melynek költségarányát az 1. számú Táblázat jól mutatja. Az egységes infrastruktúra kivitelezése egyértelműen és átláthatóan bemutatható ábrákkal, melyek megyei, régiónkénti és országos bontásban utalnak a megvalósítandó egységes hálózati infrastruktúrára és szolgáltatásaira, úgy hogy magukban foglalják a gerinchálózat és a készenléti szervek rendszereit is.

12. A MEGVALÓSÍTÁS INDOKAI

Magyarországon – hasonlóan a többi európai államhoz – a magyar állampolgárok és az ide látogató külföldiek alanyi jogon várják el, hogy amennyiben a biztonságuk, az egészségük, a vagyonuk veszélybe kerül, az arra hivatott készenléti szervezeteket a lehető leggyorsabban érjék el és azok a lehető leghatékonyabban, legeredményesebben segítséget nyújtsanak. Az egységes Európai Segélyhívószám (112) és az ezen a hívószámon kezdeményezett segélyhívásokat fogadó szolgálat működtetése közösségi előírás.[2]

Az előzőekből, már látható, hogy az ORFK, OKF és az OMSZ a kellő hatékonyság eléréséhez szolgálat-, bevetés- és mentésirányítási rendszerek megvalósítását tervezi, mely lehetőséget biztosít a készenléti szervezetek között élő, operatív kapcsolat megteremtésére és vészhelyzetekben az összehangolt irányításra. Tekintettel arra, hogy a készenléti szervezetek említett szolgálat-, bevetés- és mentésirányítási rendszerei országos kiterjedésűek és számos csatlakozási és végponttal rendelkeznek majd, a rendszerek megfelelő működéséhez elengedhetetlen a rendszerek és a végpontjaik közötti kommunikációt biztosító hálózati (fizikai) infrastruktúra (lásd 26 ábra KEK KH hálózati szint) rendelkezésre állása.

A kiemelkedő jelentőségű feladatokat ellátó készenléti szervezetek számára elengedhetetlen a katasztrófatűrő redundáns kerülő útvonalakat is tartalmazó adatkapcsolatok biztosítása.

Ezen túlmenően, a zRH kommunikációs infrastruktúráját jelenleg is használó szervek, szervezetek megnövekedett informatikai fejlesztésével, és a rendszereket használó végpontok számának emelkedésével párhuzamosan az adatkommunikációs igény is fokozottan változik. A változás egyrészről a megnövekedett adatmennyiség miatti sávszélesség bővítését, másrészt a megváltozott kommunikációs igények miatt a szolgáltatások módosítását idézik elő. Mindezeket figyelembe véve egyértelműen igazolható a megvalósítás.

13. A MEGVALÓSÍTANDÓ HÁLÓZAT FELADATSPECIFIKÁCIÓJA ÉS KÖLTSÉGIGÉNYE

A költségek meghatározásához nagyban hozzájárul, az elvégzendő feladatok értelmezése, ugyanakkor ez fordítva is igaz, vagyis az elvégzendő feladatok értelmezése segít a költségek meghatározásában. Mivel a megvalósítás egy komplex hálózati infrastruktúrát vázol, így a zRH infrastruktúrával szorosan összefüggő fejlesztések illetve az üzembe állítás költségeivel is számoltunk. Ezeket azonban nem forintosítottuk, hanem százalékos megosztást alkalmaztunk, ahol a teljes megvalósítás költsége 100%.

Az alábbi táblázatban a fejlesztés költségmegoszlása látható.

2 Az Európai Parlament és a Tanács 2002. március 7-i 2002/21/EK irányelve az egyetemes szolgáltatásról és az elektronikus távközlési hálózatokhoz és szolgáltatásokhoz kapcsolódó felhasználói jogokról

Feladat csoport	Költség (100%)	Megjegyzés
Követelmények specifikálása	0	Folyamatos együttműködés és egyeztetés a készenléti szervezetekkel
Központi gerinchálózat fejlesztése	70	
ORFK, OKF, OMSZ gerinchálózaton kívüli végpontjainak csatlakoztatása, integrálása	25	
Üzemeltető személyzet felkészítése, oktatás	2	
Infrastruktúra tesztelése, kiemelt rendelkezésre állási időszak	2	
Egyéb	1	Pl.: Előkészítés, Projektmenedzsment, minőségbiztosítás

1. táblázat: A megvalósítás költségmegoszlása

14. NEMZETKÖZI KITEKINTÉS

Európai viszonylatban működik az EENA – European Emergency Number Association (Európai Segélyhívószám Egyesület), mely 1999-ben alakult és jelenleg 125 tagja van. Alapvető célkitűzése annak a problémakörnek a feloldása, mely abban rejlik, hogy a készenléti feladatok szabályozása és végrehajtása nemzeti, a távközlési feladatoké pedig Európai Uniós hatáskörbe tartozik. Az ebből fakadó érdekellentétek, problémák ügyében közvetít az EENA, azaz a nemzeti szervek „hangját” igyekszik képviselni Brüsszelben.

Az országok között változatos megoldások alakultak ki a 112-esen alapuló Egységes Segélyhívó Rendszerre és az egyes országok különböző felkészültségi szinten állnak a kérdést illetően. Egy valamiben azonban közös teendőik vannak, mégpedig a 112-es hívószám ismeretének terjesztésében, hiszen elmondható, hogy csupán a lakosság negyede ismeri a 122-es számot. A segélyhívások fogadása során szinte mindenhol nehézségbe ütközik a többnyelvűség, melynek megléte elengedhetetlen a hatékony segítségnyújtás érdekében.

Áttekintés képen elmondható, hogy néhány ország olyan modellt alkalmaz, ahol a híváskezelést valamelyik készenléti szervezet (jellemzően a rendőrség) végzi (Ausztria, Németország, Franciaország, Olaszország). További megoldásokat jelentenek a beérkező hívások előszűrését végző szervezeti esetek (Egyesült Királyság, Írország, Hollandia). Más országokban (pl. Belgiumban) ezt a funkciót integráltan kialakított körletben végzik a közreműködő egységek, ahol azok egy közös helyszínen helyezkednek el. További eltérő (talán magasabb szintű) működési modellt jelent, amikor a segélyhívás fogadását és annak diszpécseri kezelését egy jól képzett személyzettel rendelkező egység végzi, megfelelően kialakított erőforrás-háttérrel (Finnország, Svédország). Ezektől a hierarchiáktól teljesen eltérő szövevényes kapcsolati rendszerben működik a Csehországban és Bulgáriában kialakított rendszer, ahol mindenki szinte mindenkivel hálózati kapcsolatban van.

Most néhány országot az elérhető információk alapján mutatok be a teljesség igénye nélkül.

A Cseh Köztársaságban – a közigazgatási beosztásnak megfelelően – 14 szolgáltató központ üzemel, amelyek közül 3 helyszín magasabb prioritási szintet képvisel és egyben a regionális központok foglaltsága, vagy egyéb elérhetetlensége esetén szekunder fogadó és intézkedő helyszínt jelent.

A telekommunikációs rendszer által továbbított, a helymeghatározásra vonatkozó pozícióinformációk a CCITT SS7 jelzésrendszer részeként továbbítódik a feldolgozó központba, akár szekunder feldolgozás esetében is.

A rendszer kiépítése során olyan fő paramétert vettek figyelembe, hogy a segélyhívást kezdeményező személy a gépi hívásfogadástól számított 4-5 másodpercen belül elérje az élőbeszéddel jelentkező diszpécsert.

Szlovákiában a különféle eszközök alkalmazását tartják célszerűnek, beleértve a szervezési optimalizálásokat, a szervezetek kapacitásának (személyzetének) növelését, a minőségbiztosítást, valamint integrált, közös kommunikációs infrastruktúra kialakítását. Tapasztalataik szerint a lakosság körében az ismeretek szélesítésével jelentősen csökken a rosszindulatú, illetve a téves híváskezdeményezések száma.

Lengyelországban, azaz Krakkóban és környezetében, mintegy 1,1 millió lakost kiszolgáló úgynevezett pilot rendszer működik, ahol a beérkező mintegy napi ezer hívás lekezelését igen gyorsan, átlagosan kevesebb, mint 5 másodperc várakozási idő alatt végzik. A hívások fogadása során háromnyelvű kezelésre is felkészültek.

Litvánia mintegy 3,5 millió lakosú országában naponta körülbelül 4000 hívás kezelésére van szükség. A helymeghatározásra vonatkozó információk pontossága rendkívül változó (50 m-től akár 10 km-ig, a rendkívül nagy léptékű információ azonban a semminél még mindig több). A készenléti szervek a TETRA technológiát alkalmazzák.

Hollandiában a rendszer bevezetése több mint 10 évet vett igénybe (több közbülső egységesítési törekvésen keresztül). Fontos tapasztalatként leszűrhetjük, hogy a segélynyújtás rendszerének kialakításakor igen eltérő szempontokat is mérlegelni kellett. Jelentősen eltér a segélyhívást kérő fél, valamint a kiszolgálást végző személyzet megközelítési módja, ami teljességgel érthető, figyelembe véve például a pánikhelyzetet is. A My-SOS fantázia nevű rendszer mintegy 4 éve működik az országban, csaknem 8000 db készülékkel, amelybe előre be lehet programozni megadott hívószámokat, köztük a 112-t is. A készülék a segélyhívás kezdeményezésekor az aktuális GPS adatokat is bemondja. (A rendszer üzemeltetése piaci alapon történik.)

Romániában korábban decentralizáltan működött a segélynyújtást. Jelenleg a Speciális Telekommunikációs Szolgálat keretein belül fogadják a 112 segélyhívásokat. A segélyhívó rendszert az egységesítés során a közigazgatási tagozódásnak megfelelően alakították ki. A végrehajtó állomány IP alapú adatátviteli hálózatot és zömmel TETRA technológiájú rádiókommunikációt használ, de működnek még a hagyományos analóg rendszereik is. Jövőbeni legfontosabb feladataiknak a különféle részterületek szabványosítását, a reagáló-képesség fokozását, valamint a kiszolgáló személyzet speciális tudásának (nyelvi képességek, specifikus szakmai – pl. vegyi, biológiai, stb. – ismeretek) fejlesztését tekintik.

Angliában, konkrétan a Londoni Mentőszolgálatnál mintegy 7 millió lakos kiszolgálása a feladat. A nagyszámú eseteket 3 kategóriába sorolják, életveszélyben van, sérülés történt, de nincs életveszély, és a hívó segítséget igényel. Tapasztalataik azt mutatják, hogy manapság a segélyhívás kezdeményezésének helyszíne – amire a helymeghatározás adata vonatkozik – sok esetben, teljes mértékben eltér a segítségnyújtásra vonatkozó igény földrajzi helyétől. Régebben a segélyhívás kizárólag onnan érkezett, ahol éppen a segítségkérő is tartózkodott. Manapság azonban bárhonnan, akár külföldön tartózkodó rokontól is érkezhet. Ebben az esztendőben a londoni mentők már több alkalommal fogadtak segélyhívást Franciaországból, Hollandiából, az Egyesült Államokból, sőt Ausztráliából is olyan esetben, amikor Londonban volt valakinek szüksége segítségre. Náluk mutatkozik meg leginkább a nyelvi nehézség kezelésének problematikája is. A jelenséget a nagyarányú migráció következményeként értékelték, amelyből adódóan a hívások jelentős arányánál nem anyanyelvi angol nyelven indul a kommunikáció. Néhány meglepő adat egy iskolai felmérésből, mely az elsődleges nyelv-előfordulási arányokat mutatja: angol - 72%; bengáli - 5%; pandzsábi - 4%; hindi - 3%; török - 2%; arab, joruba, szomáli is 1 - 1 %.

A madridi 112-es szervezetben is a többnyelvűség problémaköre emelhető ki.

Szervezetükben a hívásfogadók között alkalmazási feltétel az angol nyelv megfelelő ismerete, de sok esetben második nyelvet is tudnak (német, francia vagy akár román, kínai, japán stb.). A hívás-fogadás folyamatának első lépéseként a segélykérés nyelvét kell

azonosítani. Amennyiben a hívás anyanyelven, vagy angolul érkezik, akkor a hívást fogadó állomány saját maga végzi a folyamat lekezelését. Amennyiben olyan nyelven történik a segélykérésre vonatkozó hívás (pl. angol vagy francia), amelynek ismerője szolgálati váltásban dolgozik, akkor a hívás átirányításra kerül hozzá. Egyéb problémás esetekben tolmács segítségét veszik igénybe akár konferencia beszélgetésként is.

A spanyolok bemutattak egy olyan alkalmazást, mely a segélynyújtás során a képi információk fontosságára fókuszál. A rendszer képes a telekommunikáció új lehetőségeit kihasználva képi információk továbbítására is, mely veszélyhelyzetben a reagálást döntően befolyásolja, hiszen pontosabb, képi információ is rendelkezésre áll. A rendszer lehetővé teszi, hogy már a bejelentkezéskor az erre alkalmas mobil telefonokkal a képfelvétel is továbbításra kerüljön a segélyhívó központba, valamint a megindult segélynyújtás idején is lehetőség van a képek továbbítására.

A fenti példákból jól látható, hogy mindenhol működik valamilyen szintű egységes katasztrófavédelem, melyek ugyan eltérő módszereket és technológiai megoldásokat alkalmaznak, de működőképesek. Azt gondoljuk, más országoktól némi tapasztalatot meríthetünk a megoldásra vonatkozóan, megismerhetjük nehézségeiket, ötletet kaphatunk egy-egy probléma megoldására. Azonban látnunk kell, hogy az optimális megoldást nekünk, saját magunknak kell megtalálnunk. Ehhez - a fentieket is megfontolva - fordítsunk nagyobb hangsúlyt az alábbiakban összefoglaltakra:

- Minden erőfeszítést meg kell tenni az egységes integrált segélynyújtást irányító rendszerek kialakítására és a szükséges források biztosítására.
- Fokozatosan bővíteni kell a helymeghatározásra vonatkozó, rendelkezésre álló adatok fogadását, a lehetőségeknek megfelelő alkalmazását, figyelembe véve, hogy a költség-hatékony megoldásokból adódó korlátozott pontosság is jobb az információ hiányánál.
- Célszerű lenne kialakítani a 112 hívásfogadást biztosító integrált szervezetet, akár a készenléti szervek bázisán, akár az államigazgatás egyéb szintjén.
- Reméljük, hogy ezen nemzetközi példákkal sikerül előmozdítani a készenléti szervek együttműködését.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az egységesített infokommunikációs hálózati infrastruktúra kivitelezése a legegyszerűbb és legkézenfekvőbb megoldási módot nyújtja, amelyet az egyeztetések, konzultációk során az érintettek is támogatásra méltónak ítéltek.

A közleményben megfogalmazottak bevezetése elősegítheti, hogy a készenléti szervezetek a kérdés kapcsán egy platformra kerüljenek, valamint egyértelművé válhat az is, hogy az egységesítés szükségessége és kivitelezhetősége egyben egy optimális megoldási alternatívát is kínál. Az elkövetkezőkben kidolgozásra vár még a témához kapcsolódó oktatatás és üzemeltetés területe.

Konklúzióként megfogalmazható, hogy az érintett szervezetek specifikuma, szervezetük struktúrája nagyban befolyásolja együttműködésüket, szakmai feladataik szervezését, operatív tevékenységeik végrehajtását. Ezek jelenleg nem tisztázottak, és nem teljesen egyértelműek. Ennek rendezését elsődlegesen törvényi, jogszabályi szinten célszerű megoldani. Minden más, például a 112 hívószámon alapuló ESR rendszer egységesítésének a kérdésköre és annak infokommunikációs háttere csak ennek függvényében kivitelezhető. Addig a szervezetek feladatuk ellátása érdekében saját maguk, megítélésük és egyéni szempontjaik prioritásával végzik el a szükséges fejlesztéseket. Azonban, ameddig ezek a feltételek nem változnak, nem teremtődnek meg, az adott lehetőségek kihasználását szem előtt tartva racionalizálni, erősíteni kell a szervezetek közötti együttműködést, támogatni az

erre irányuló törekvéseket nem utolsó sorban realizálni, véghezvinni magát az egységesítést. Amennyiben az érintettek a megoldáskereső gondolkodásmódot és hozzáállást követik, szélesíthetik spektrumaikat és könnyíthetnek nehézségeiken. Mindezek fontosságát és az adott lehetőséget felismerve, az érintettek egyre inkább hajlanak az egységes hálózati infrastruktúra megvalósítására.

FELHASZNÁLT IRODALOM

[1] Tanka László: Az EKOP kiemelt projekt célrendszere és tartalmi elemei – A rendőrség 112-es segélyhívó ügyeleti és szolgálatirányítást támogató rendszerének komplex országos fejlesztése, http://kvk.bmf.hu/emcom2009/doc/tanka_laszlo.ppt (2010-04-09)

[2] Országos Katasztrófavédelemi Főigazgatóság: Bemutatkozás, Szervezet, Jogszabályok, http://www.katasztrofavedelem.hu (2010-04-09)

[3] Egészségügyi Stratégiai Kutatóintézet: Egészségpolitikai fogalomtár, http://fogalomtar.eski.hu/index.php/Kezd%C5%91lap (2010-04-10)

[4] Bartha István-Dr. Simon Marianna: Az OMSZ mentésirányítási rendszere (MIR) EMCOM 2009 Hévíz, http://kvk.bmf.hu/emcom2009/doc/bartha_simon.ppt (2010-04-15)

[5] Országos Mentőszolgálat: Az OMSZ szolgálatvezetésének korszerűsítési terve, http://www.mentok.hu/page.php?newmenuid=63 (2010-04-15)

[6] Országos Mentőszolgálat: Az Országos Mentőszolgálat Működési szabályzata Budapest 2006, http://www.mentok.hu/file.php?type=showpage&file_id=11 (2010-04-18)

[7] Dr. Göndöcs Zsigmond - Dr. Simon Marianna - Bartha István-: Az OMSZ mentésirányítási rendszere (MIR) Professzionális Mobil Távközlési Nap 2010-04-15, http://www.pro-m.hu/resource.aspx?ResourceID=gondocs3 (2010-04-20)

[8] PRO-M Zrt.: EDR Nap 2010 Konferencia anyagok 2010. 04. 20. http://www.pro-m.hu/engine.aspx?page=showcontent&content=EDR2010NAP (2010-04-20)

Kendernay Zsolt – Takács Attila – Pándi Erik – Rajnai Zoltán
kendernayz@mail.ahiv.hu – attila.takacs@mail.ahiv.hu – pandi.erik@zmne.hu – rajnai.zoltan@zmne.hu

A KÖZIGAZGATÁSI ÉS ELEKTRONIKUS KÖZSZOLGÁLTATÁSOK KÖZPONTI HIVATALA (KÖZPONTI HIVATAL) SZEREPE AZ EGYSÉGES SEGÉLYHÍVÓ RENDSZER KIALAKÍTÁSÁBAN[1]

Absztrakt

Jelen közlemény a KEK KH 112 rendszer kialakításában játszott feladatrendszerét tekinti át.

This publication studies the role of KEK KH in the establishment of the 112 Emergency System.

Kulcsszavak: *KEK KH, Egységes Segélyhívó Rendszer (112) ~ KEK KH, 112 Emergency System*

BEVEZETÉS

A Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEK KH) a Miniszterelnöki Hivatalt vezető miniszter irányítása alá tartozó önálló szervezet. A miniszter külön jogszabály alapján, az infokommunikációért felelős kormánybiztos útján gyakorolja az irányítási jogát. A KEK KH a feladat- és hatáskörébe tartozó közigazgatási ügyekben hatósági jogkörrel felruházott, önállóan gazdálkodó költségvetési szerv. Az Egységes Segélyhívó Rendszer (ESR) működésére vonatkozó szerepét a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről szóló 276/2006. (XII. 23.) Korm. rendelet definiálja.

1. A KEK KH FELADATAI

A hivatal 112-es hívószámra alapozott ESR-rel kapcsolatos feladatai a következők:[2]

- Közreműködik az elektronikus közigazgatás koncepcióban megfogalmazott kormányzati stratégiai célok megvalósításában;
- a közigazgatási informatikával, illetve a közigazgatási szolgáltatások korszerűsítésével összefüggő feladatai körében ellátja a rendeletben meghatározott feladatokat;
- az egységes digitális rádiótávközlő rendszerről szóló 109/2007. (V. 15.) Korm. rendelet, valamint a zártcélú távközlő hálózatokról szóló 50/1998. (III. 27.) Korm. rendelet alapján ellátja a rendeletben meghatározott telekommunikációs és hálózat-fenntartási feladatokat.

A hivatalon belüli konkrét feladat ellátását a volt BM Távközlési Szolgálat (BM TÁSZ), azaz jelenlegi nevén az Adathálózati és Távközlési Főosztály (ATF) végzi.

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült
2 Forrás: http://www.nyilvantarto.hu/kekkh/kozos/index.php?k=hivatalunkrol_hu_feladatok

1.1. Adathálózati és Távközlési Főosztály (ATF) feladatai, szolgáltatásai

A főosztály, mint a BM TÁSZ jogutódja magával hozta, megőrizte és kibővítette feladatkörét, melynek része a 112-es hívószámon alapuló ESR rendszer is, amelynél ellátja a tevékenységirányító rendszerek együttműködésének segítését a rendészeti hálózaton belüli integrációját és az ebből következő üzemviteli feladatokat. Infokummunikációs szempontból profiljába tartozik az Elektronikus Kormányzati Gerinchálózat (EKG) alhálózataként működő zárt rendészeti hálózat (zRH) üzemben tartása, adatkapcsolati átjáró biztosítása az EKG-n keresztül az érintett intézmények informatikai rendszeréhez. Országos távközlő rendszerei révén feladatkörébe tartozik továbbá a nemzetbiztonsági, igazságszolgáltatási, rendvédelmi, illetőleg védelmi igényeket kielégítő szervek részére nyújtandó távközlési és adatátviteli szolgáltatások nyújtása. Ellátja még az EDR használatát biztosító virtuális magánhálózat (VPN), valamint a központi menedzsment üzemeltetését. Biztosítja a Hivatal a katasztrófavédelemmel és a katasztrófatűrő képesség kialakításával összefüggő hírközlési feltételeket. Kapcsolatot tart a közcélú távközlési szolgáltatókkal a készenléti, gazdaságmozgósítási feladatok ellátása érdekében.

1.2. A zRH által biztosított szolgáltatások

A meglévő infrastruktúra jelenleg a következő szolgáltatásokat biztosítja a kapcsolódó szervezetek számára:

- MPLS alapú IP VPN szolgáltatás;
  - a technológia lehetővé teszi, a virtuális magánhálózatok kialakítását.
- Optikai hálózatra épülő Gigabit Ethernet szolgáltatás;
  - Budapestre lett kialakítva, ahol a központi berendezések 10 Gbit/s sávszélességgel vannak összekötve.
- IPSec VPN szolgáltatás;
  - Az IPSec a kommunikációban résztvevők hiteles azonosítását és az adatforgalom kódolását biztosítja;
  - A VPN központon keresztül a szervezetek elérik saját virtuális hálózati infrastruktúrájukat.
- IP alapú telefon szolgáltatás;
  - A rendszer lehetővé teszi távoli szervezetek részére is Voice-Gateway keresztül az IP telefon hálózathoz való csatlakozást.
- Analóg telefon szolgáltatás;
  - analóg vagy digitális készüléken telefon és faxszolgáltatás biztosít. Rendelkezik kijárattal a nyilvános telefonhálózat irányába és kiszolgálja a 112-es hívószámra beérkező segélykérő telefonokat.
- Hálózat menedzsment;
  - a szolgáltatás az üzemeltetői személyzet munkáját, valamit a kapcsolódó szervezetek üzemeltetői számára, a hálózati hibák, felderítését segíti.

1.3. Az ATF hálózati infrastruktúrája

A zRH hálózati infrastruktúrája több egymással szorosan összefüggő részre bontható.

Országos mikrohullámú gerinchálózat

- a magas rendelkezésre állást a kétirányú összeköttetés, a nagy sávszélességet a központi objektumok közötti - Hármashatár-hegy, Kab-hegy, Galyatető, Misinatető

és Kiskunfélegyháza - 155Mbps (STM-1) a felhasználó szervezetekig nx2 Mbps sebesség biztosítja.

MPLS technológiára épülő országos kiterjedésű szolgáltatói hálózat

- Leegyszerűsíti az útvonalválasztást, valamint lehetővé teszi a sávszélesség értékekének igény szerinti megadását.
- A magas szintű rendelkezésre állás és hibatűrés érdekében a végponti eszközök lehetőség szerint legalább két központi kapcsolóra csatlakoznak.
- Az alkalmazott OSPF dinamikus routing protokoll az adatkapcsolatok forgalmát egyszerűsíti.
- A Quality of Service (QoS) szolgáltatás a szervezetek forgalmát optimalizálja, mivel a QoS képes a hálózatok és hálózati eszközök erőforrásainak meghatározott rend szerinti felosztására, és a garantált sávszélesség biztosítására. A technológia a magas prioritású üzeneteket előnyben részesíti alacsonyabb besorolású társaikkal szemben, és konkurencia-helyzetben előbbiek továbbítása, utóbbiak feltartóztatásával garantált sebességen biztosítható.
- A szervezetek részére a MPLS VPN technológia biztosítja a virtuális magánhálózat előnyeit.

Budapestet lefedő, Ethernetkapcsolókra épülő Gigabit Ethernet gerinchálózat

A budapesti gerinchálózat öt kulcsfontosságú objektum köré épül:

- ORFK székház (Teve utca);
- Önkormányzati Minisztérium központi épülete (József Attila utca);
- KEK KH zRH központi objektuma (Hármashatár-hegy);
- KEK KH Balázs Béla utcai központja;
- KEK KH Róna utcai központja.

Az ORFK székház, a Róna utca és a Balázs Béla utca telephelyek 10 Gbps sávszélességgel vannak összekötve. A többi objektum Ether-Channel 2Gbps kapacitással kapcsolódik egymáshoz.

A redundáns kapcsolatokat az úgynevezett hurkok kialakítása adja, ami azt jelenti, hogy több objektum egymás után fűzve csatlakozik két központi kapcsolóhoz. A csatlakozó szervezetek objektumai számára 10Mbps, 100Mbps vagy Ether-channel technológiával akár a 800Mbps sávszélességű összeköttetés is biztosított.

Az objektumok forgalmának elkülönítését a virtuális LAN (VLAN) technológia oldja meg.

A budapesti gerinchálózat és az országos MPLS hálózat között a kapcsolat a Hármashatár-hegyen valósul meg. A budapesti Gigabit Ethernet gerinchálózat Ethernet kapcsolói és az országos szolgáltatói hálózat központi routerei egy-egy Gigabit Ethernet interfésszel kapcsolódnak egymáshoz.

A távoli bejelentkezést biztonságosan megvalósító VPN központ

A VPN központ szerves részét képezi mind az országos gerinchálózatnak, mind a budapesti gerinchálózatnak. A VPN központ alkalmas mobil felhasználók által indított IPSec VPN kapcsolatok fogadására (remote access VPN), külső intézményekkel, szervezetekkel

pont-pont IPSec kapcsolatok kialakítására, valamint a zRH hálózati infrastruktúrájához kapcsolódó szervezetek telephelyi VPN kapcsolatainak kiszolgálására.

IP alapú telefonhálózat

A Hármashatár-hegyi objektumban egy Cisco IP telefon rendszer áll rendelkezésre, mely Voice-Gateway keresztül kapcsolódik a KEK KH analóg telefon hálózatához.

Az IP telefon viszonylag kis kapacitású adathálózaton is képes megfelelő hangszolgáltatásra. A tömörített eljárásnak köszönhetően csak 8 Kbps foglal a kapacitásból.

A zártcélú Rendészeti Hálózat (zRH) a jogszabályi előírások értelmében az Elektronikus Kormányzati Gerinchálózat (EKG) alhálózatának tekinthető. A zRH infrastruktúrája az EKG infrastruktúrájától teljes mértékben független. Míg az EKG optikai kapcsolatokra épül, addig a zRH mikrohullámú összeköttetéseket alkalmaz. Az eltérő kommunikációs kapcsolatoknak és a független eszközparknak köszönhetően a két hálózat egymást jól kiegészíti, így a készenléti szervezetek számára, - akiknek elengedhetetlenek a hibatűrő adathálózatok és távbeszélő szolgáltatások - optimális megoldást biztosítanak.

2. A KEK KH VÁRHATÓ FEJLESZTÉSI IRÁNYA

A hivatal zRH hálózat fejlesztését elsősorban a készenléti szervezetek részéről felmerült igények határozzák meg, amelyet a hivatal pályázatok révén kíván megvalósítani. A készenléti szervezetek tervezett fejlesztései jól tükrözik a szolgáltatásokkal szembeni elvárásaikat. Mint láttuk az OKF célja, hogy a katasztrófavédelemben résztvevő szervezetek között gyors, megbízható és minden körülmények között működő informatikai rendszer valósuljon meg. Az ORFK szándéka egy olyan szolgálat-irányítási rendszer, amely krízishelyzetben elektronikus módon képes az információt fogadni, feldolgozni és továbbítani az illetékes központ felé. Az OMSZ bevetés-irányító rendszere veszélyhelyzetben a digitális hálózat nyújtotta lehetőségekkel kíván élni.

Ahhoz, hogy a zRH a megnövekedett igényeknek megfelelő infrastruktúrával rendelkezzen, a következő fejlesztéseket kívánja végrehajtani.

- Nagysebességű, megbízható távközlési adatkapcsolatok bővítése Budapest területén szervezetenként minimálisan 100Mbps csatlakoztatási lehetőséggel;
- Nagysebességű, megbízható távközlési adatkapcsolatok fejlesztése régiós illetve megye viszonylatokban, szervezetenként minimálisan 2-50Mbps csatlakoztatási lehetőséggel;
- Az szervezetek nagytávolságú hálózati infrastruktúrájában magas rendelkezésre állás megvalósítása, szükséges tartalékolások beiktatása, redundancia megteremtése;
- Digitális telefonhálózatok, telekommunikációs rendszerek átjárhatósága, összekapcsolása, egységes IP protokoll alapú tartalék útvonal és hívás irányítás lehetőségének kiépítése;
- Szervezetek közötti közös informatikai szolgáltatások lehetőségének megteremtése;
- Mobil-internetes és internetes felhasználók biztonságos kiszolgálása preferált IPSec VPN központ és szigorú authentikációs eljárások;
- Egységes hálózatmenedzsment és HelpDesk szolgáltatás, valamint üzemeltetési háttér;
- Egységes hívásfogadó diszpécser állomások kialakítása, hívás információk rögzítése;
- EDR kapcsolódási pontok kialakítása, központi VPN együttműködés kialakítása.

Megvalósítandó műszaki, infrastrukturális fejlesztések

A tervezett szolgáltatások megvalósításához a zRH alábbi területeit kell vizsgálni és a szükséges fejlesztéseket elvégezni:

- Országos mikrohullámú és budapesti optikai gerinchálózat;
- Megyei felhordó hálózatok bővítése, korszerűsítése;
- Országos MPLS hálózat és budapesti Gigabites hálózat;
- A hálózaton megvalósuló TDM over IP rendszer bővítése;
- Digitális távbeszélő hálózat és IP alapú távbeszélő szolgáltatás bővítése;
- IP alapú hívásirányítás kialakítása;
- VPN központ és authentikációs megoldások bővítése;
- Help-Desk és felügyeleti rendszerek korszerűsítése;
- Hálózat rendelkezésre állásának növelése, tartalékolások kialakítása, redundáns eszközök alkalmazása;
- Hálózatbiztonsági kockázatok csökkentése, kizárása.
- Mint a leírtakból kiderül, a KEK KH zRH jelenlegi hálózata rendelkezik egy alapstruktúrával, mely továbbfejlesztve még inkább alkalmassá teszik, hogy a készenléti szervezetek számára a kor igényeinek megfelelő műszaki, infrastrukturális, országos lefedettségű átviteltechnikai hálózatot biztosítson.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A zRH célja olyan szolgáltatás nyújtása, ahol a hálózatra kapcsolódó szervezetek, az ügyintézéshez, feladataik ellátásához szükséges input és output adataikat zökkenőmentesen és gyorsan tudják továbbítani egymás rendszerei felé. A segélynyújtási szolgáltatások esetében ez egy több szervezeten átnyúló folyamat, hiszen egy feladat végrehajtása esetenként több szervezetet is érinthet, így az adatok párhuzamos, gyors, biztonságos továbbítása kiemelten fontos.

A kommunikációs infrastruktúrának (fizikai) köszönhetően lehetőség van a szervezeteken átívelő folyamatok megvalósítására, elősegítve ezzel azt, hogy egy operatív feladat végrehajtásakor az input és output adatok mindig időben és a megfelelő helyre jussanak el, és a szervezetenként elkülönülő rendszerek egy komplex készenléti rendszerré válhassanak. Fontos megemlíteni, hogy a KEK KH a zRH-n keresztül a szervezeteknek csak magát a fizikai, hálózati infrastruktúrát szolgáltatja és a fejlesztésnek nem célja a kapcsolódó szervezetek alkalmazás szintű összekötése. A rendszerek egymáshoz való alkalmazásszintű kapcsolódását, és a folyamatok kidolgozását a szervezeteknek maguknak kell megoldaniuk saját e célra irányuló projektjeik keretében.

FELHASZNÁLT IRODALOM

[1] Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala: Hivatalunkról, http://www.nyilvantarto.hu/kekkh/kozos/index.php?k=hivatalunkrol_hu (2010-04-06)

[2] Eötvös József Főiskola: polgári védelem, http://www.ejf.hu/hefop/tantargyak/polgari_vedelem/polgari_vedelem.html (2010-04-06)

[3] Tetra Forum Hungary egyesület: A magyarországi készenléti szolgálatok távközlési helyzete,

http://www.tetraforum.hu/letoltes/20050623tfh/Amagyarorszagikeszenletiszolgalatoktavkozlesihelyzete.ppt (2010-04-08)

[4] Polgári védelem Sárvár: Polgárvédelmi fogalmak, http://w3.enternet.hu/pvsarvar/html/pv_fogalmak.html (2010-04-08)

[5] EDR – a készenléti szervek szolgálatainak nélkülözhetetlen háttér-technológiája 2009. 12. 23. http://pro-m.hu/engine.aspx?page=showcontent&content=bizt2009 (2010-04-09)

[6] Dr. Sárközy Ferenc: Térinformatika, http://gisfigyelo.geocentrum.hu/sarkozy_terinfo/t38.htm (2010-04-09)

Kerti András – Pándi Erik – Töreki Ákos
kerti.andras@zmne.hu – pandi.erik@zmne.hu – toreki.akos@zmne.hu

A VEZETÉSI ÉS INFORMÁCIÓS RENDSZER TECHNIKAI ALRENDSZERÉNEK IRÁNYÍTÁSA[1]

Absztrakt

Jelen közlemény a vezetési és információs rendszereket kiszolgáló technikai alrendszer irányítási kérdéseivel foglalkozik.

This publication deals with the questions related to the management of technical subsystem of the Command and Information System

Kulcsszavak: *információtechnológia, Magyar Honvédség, VIRTAR ~ information technology, Hungarian Defence Forces, VIRTAR*

BEVEZETÉS

A vezetési és információs rendszer technikai alrendszerének (VIRTAR) irányítása nem lehet más, nem alkalmazhat más módszereket, mint a Magyar Honvédség. Másképpen fogalmazva a VIRTAR irányításának szervesen integrálódnia kell a haderő irányításába, így mielőtt a VIRTAR irányításának kérdéseit feldolgoznánk, át kell tekinteni a Magyar Honvédség irányítási rendjét.

1. A MAGYAR HONVÉDSÉG IRÁNYÍTÁSA

Hazánkban az alapvető kérdések fundamentumaként az Alkotmány szolgál, amely e kérdéskört tekintve a következőképpen fogalmaz: *„A Magyar Honvédség irányítására - ha nemzetközi szerződés másként nem rendelkezik - az Alkotmányban meghatározott keretek között kizárólag az Országgyűlés, a köztársasági elnök, a Honvédelmi Tanács, a Kormány és az illetékes miniszter jogosult."* [1]. Az Alkotmány tehát rögzíti a legfelsőbb szintű, alapvető irányítási jogosultságokat, amely mellett a Magyar Honvédségről szóló törvény részletezi a feladat- és hatásköröket. A törvényben a Magyar Honvédség irányításáról és vezetéséről a IX. fejezet rendelkezik. A jogszabály tisztázza a szolgálati elöljáró, a hivatali felettes, illetve a szakmai elöljáró, szakmai felettes fogalmát és meghatározza jogosultságaikat.

A fejezet meghatározza még a Magyar Honvédség felső szintű irányítását és vezetését, amelyet rendkívüli állapot idején a Honvédelmi Tanács, „béke" időszakban a honvédelmi miniszter hajt végre.

A törvény a vezetés és irányítás szempontjából még két fontos hivatali (parancsnoki) beosztást nevesít, úgymint a Honvéd Vezérkar főnökét (101. §), valamint a szakirányításért felelős honvédelmi miniszter által kijelölt személyt, aki a Honvédelmi Minisztérium hivatali szervezetének vezetője, de akinek a beosztását a szövegezés nem nevesíti (100. §). E jogkört a 2134/2006. (VII. 27.) Korm. határozat 3. pontja a kabinetfőnök hatáskörébe utalja. A két személy együttműködési kötelezettségét a törvény a 100. § (4) és a 101. § (5) bekezdése írja elő.

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

A Honvéd Vezérkar főnöke:

- közreműködik a Magyar Honvédség feladatainak teljesítése szempontjából fontos közlekedési és hírközlő hálózat, valamint a légi, sugárfigyelő, jelző- és riasztási rendszerek működőképességének biztosításában;
- a parancsnokságok, csapatok békeidőszaki vezetési rendszere működésének biztosítása érdekében tervezi, szervezi a híradással, az informatikával és a vezetés egyéb területeivel kapcsolatos feladatokat [2].

Az első pontban szereplő rendszerek esetében nem tekinthető egyértelműnek az, hogy milyen módon és kivel kell a közreműködést végrehajtani. A második pont tekintetében felmerül azon kérdés, amely szerint, ha a vezérkari főnök csak a katonai szervezetek békeidőszaki vezetési rendszer működése érdekében tervez és szervez, akkor ki, vagy mely szerv tehető felelőssé a minősített időszak vezetési rendszeréért.

A törvény 102-103. §-ai a katonai szervezetek középszintű irányítását a középszintű irányító szervek vagy más magasabb szintű parancsnokságok élén álló parancsnokok, a katonai szervezetek vezetését a szervezet parancsnokának hatáskörébe utalják. A parancsnok szolgálati hatásköre kiterjed az általa vezetett katonai szervezet működésének minden területére.

2. A KIADVÁNYOK, MINT A VEZETÉS ESZKÖZEI

A vezetés eszközeit szintén a jogszabályokban és az államirányítás egyéb jogi eszközeiben találhatjuk meg a honvédelmi törvény alapján. Ezek alapján a honvédelmi miniszter rendelettel és az állami irányítás egyéb jogi eszközeivel szabályozza a honvédelmi feladatok végrehajtását. A miniszteri utasításban (az állami irányítás egyéb jogi eszköze) kell meghatározni a miniszter irányítása és vezetése alá tartozó szervezetek tevékenységére vonatkozó szabályokat.

A Honvéd Vezérkar főnöke a vezetési hatáskörében parancsot, intézkedést és szakutasítást ad ki. A hivatali felettes egyedi utasítással érvényesíti az akaratát alárendeltjeivel szemben. Részükre a hatáskörébe tartozó és jogszabály által nem tiltott bármilyen utasítást kiadhat.

A legfelsőbb szinten az egyéb belső rendelkezésekről szintén a honvédelmi törvény rendelkezik, amely szerint szakutasításban kell meghatározni a Magyar Honvédség szakmai feladatai ellátásának alapvető szabályait, valamint a haditechnikai eszközök és anyagok üzemeltetésével, karbantartásával, javításával kapcsolatos szakmai-technikai szabályokat.

Intézkedésben állapíthatók meg egyes rendszeresen ismétlődő tevékenységek végrehajtásának szakmai, technikai vagy eljárási szabályai, ideértve a katonai szervezetek működési rendjének és a személyi állomány mindennapi tevékenységének általános rendezését igénylő kérdéseit. A további kiadványokról a vonatkozó HM utasítás rendelkezik, amely alapján rendelkezésünkre áll a szolgálati könyv (szabályzat és alapdoktrína), valamint a főnökségi kiadvány (lehet doktrína, állandó működési eljárások, szövetségi, illetve NATO egységesítési dokumentumok [STANAG, AP stb.], szakutasítás, műszaki leírás, lőtáblázat, kiképzési program, tankönyv, kézikönyv, módszertani és tansegédlet, jogszabályok vagy belső rendelkezések gyűjteménye, ár- és cikkjegyzék, hasonló rendeltetésű külföldi katonai és védelmi kiadványok fordítása, valamint szolgálati könyvnek nem minősülő, de a szabályozott tevékenységet elősegítő egyéb kiadvány).

Vizsgálataink alapján megállapítottuk, hogy jogszabály nem rendelkezik a különböző kiadványok egymáshoz való viszonyáról, sőt az egyes kiadványok tartalmáról sem. Így például nem tisztázott az sem, hogy mit kell tartalmaznia a szabályzatnak és mit az alapdoktrínának, mi a különbség a kettő között, milyen tárgyban kell őket kiadni. Ezen túlmenően a felsorolás nem is tekinthető teljesnek, mert hiányzik a rendszerből a stratégia.

Véleményünk szerint ebben a rendszerben is látszik az a tétovaság, amely a NATO tagságunkból adódik, átvettünk bizonyos dolgokat, de a régieket se mertük elvetni, átnevezni.

Tovább bonyolítja helyzetet a 74/2008. (HK 15.) HM utasítás, amelynek a célja egy új egységes rendszer kialakítása. Ennek az új rendszernek lenne feladata a műveleti képességek alakítása, a műveletek sikeres végrehajtása, a műveletekre való felkészülés és a kiképzés hatékonyságának növelése, a vezetői kontroll erősítése, a belső eljárásrend, az együttműködés rendszerének és a különböző vezetői szinteken jelentkező egyéb katonai feladatok végrehajtásának hatékonysága folyamatos javítása érdekében tapasztalat feldolgozó-rendszer kialakítása és működtetése [3].

A rendszer céljával alapvetően egyetértünk, a probléma véleményünk szerint abban fogalmazható meg, hogy ismételten átvettünk egy működő rendszer egyetlen darabját lényegi kritikai észrevétel nélkül. A tapasztalat-feldolgozó rendszerben tetten érhető az amerikai precedens rendszer, amely azt jelenti, hogyha már volt ilyen tapasztalatunk, akkor azt alkalmazzuk is. Az utasítás lényegében nem rendelkezik arról, hogy a tapasztalati rendszer hogyan illeszkedik a már meglévő vezetési rendszerünkhöz. Az előzőekben már említett, egyes szemszögből kaotikusnak aposztrofálható rendszer már meglevő rendszerekhez fűződő viszonyát tovább bonyolítja az egymáshoz rendezés tisztázatlansága. Felmerülhet továbbá a kérdés, hogy a meglévő, a még ki nem vont nemzeti, vagy a NATO által kiadott dokumentumot használjuk, vagy csak egyszerűen alkalmazzuk a tapasztalat-feldolgozó rendszer adatait.

Azt, hogy a felvázolt probléma nem csak nemzetünk sajátja mutatja jól, hogy a szövetségesi rendszerünkben kiemelt feladatként kezelik a különböző területek interoperabilitási kérdéseit. Adminisztratív területen, a szabályzók kiadásakor is törekednünk kellene az interoperabiltiás megvalósítására. Erre a felsőszintű akarat meg van az egyik irányból, amikor a NATO előírások hazai alkalmazásának kérdéseit érintjük. A másik irányból tekinthető problémának azon tény, amely szerint saját előírásainkat kellene úgy kidolgozni, hogy azok megfeleljenek a NATO követelményeknek, azonban a megvalósítás elrendelésére nem találtunk kézzel fogható utalást sem a jogszabályok, sem az állami irányítás egyéb jogi eszközei között.

A különböző szakterületek szabályozását előíró NATO dokumentumok legtöbbje beleilleszthető egy négyes sémába, amelynek az elemei a politikák, direktívák, irányelvek, valamint egyéb támogató dokumentumok. Amennyiben a vezetési és rányitási dokumentumainkat kompatibilisé akarjuk tenni a NATO-val, két lehetőségünk van:

- a jelenlegi rendszert teljesen felülbírálva, a NATO terminológiát alkalmazzuk, amely azonban nagyon nagy, egyszer elvégzendő munkát jelent;
- a jelenlegi rendszert változatlan formában hagyjuk meg, viszont a már meglévő belső utasításainkat megfeleltetjük a NATO ekvivalens dokumentumaival.

A feladat végrehajtása nem tekinthető egyszerű feladatnak, mert vannak olyan szabályzataink, amelyek nem csak egy NATO dokumentum szintnek felelnek meg hanem többet is felölelhetnek.

3. A VIRTAR IRÁNYÍTÁSA

A szakirányítást végző személy (szakterületén a szakmai felettes vagy elöljáró), illetve szervezet feladatai a következőképpen foglalhatók egybe:

- belső rendelkezéseket ad ki a jogszabályok és az állami irányítás egyéb jogi eszközei végrehajtására;

- intézkedik a szakmai tevékenység végrehajtásával kapcsolatban, a közvetlenül alárendelt szervezetek, illetőleg a Magyar Honvédség szaktevékenységet ellátó szerveire vonatkozóan;
- feladatkörébe tartozó információkat ad és kér;
- szakterületének körébe tartozó jogszabályokat és döntéseket készít elő;
- véleményezési jogot gyakorol;
- ellenőrzi az alárendelt szakmai szervezetek tevékenységét, illetőleg – a miniszter nevében és megbízásából - az alárendelt katonai szervezetek parancsnokainak és más szolgálati elöljáróinak szakmai tevékenységét;
- a szakterületéhez tartozó, általa irányított tevékenység egységes gyakorlatának kialakítása érdekében dönt a végrehajtás során felmerült vitás kérdésekben, illetőleg állásfoglalás kiadásával biztosítja a szakmai feladatok egyöntetű végrehajtását [4].

A VIRTAR szakmai vezetése egy fontos dologban különbözik a többi szakmai tevékenységben méghozzá abban, hogy nem csak a szakmai alárendeltek feladatait kell vezetnie, hanem felügyelnie kell egy működő rendszert is. E tevékenységekről az Összhaderőnemi Doktrína meghatározza, hogy a híradó és informatikai rendszer vezetése magában foglalja a hadműveleti és az üzemeltetést irányító funkciókat. A hadműveleti vezetés a rendszer tervezőszervező tevékenységét foglalja magában és a híradó és informatikai irányító pontról történik. A rendszer üzemeltetésével (fenntartásával, kiszolgálásával) kapcsolatos tevékenység a hálózat-felügyeleti központból valósul meg.

Figyelembe véve azonban azt, hogy a jelenleg is üzemelő hálózataink (híradó, valamint az informatikai) korszerű átviteli szabványokra alapulnak [5], illetőleg a NATO szakemberei gyakorlatilag a hálózat nyújtotta képességek erőteljes továbbfejlesztésében gondolkodnak, a Magyar Honvédségben is szükséges létrehozni a számítógép veszélyjelző és incidenskezelő központot, NATO terminológiát használva CIRC-et.

4. JAVASLAT A VIRTAR TERVEZŐ ÉS SZERVEZŐ MUNKA IRÁNYÍTÁSÁNAK KIALAKÍTÁSÁRA A MAGYAR ÉS NEMZETKÖZI SZABVÁNYOK ALAPJÁN

Véleményünk szerint a Magyar Honvédség előtt álló fejlesztési feladatok, vagyis a hálózatközpontú környezetben való alkalmazás képességének kialakítása megköveteli a VIRTAR korszerű szemléletű vezetésének bevezetését. Bármiféle vezetési rendszert is alakítunk ki célszerű azt írásban rögzíteni. Erre azért is szükség lehet, mert az elmúlt évek tapasztalatai alapján kijelenthető, hogy bármely szervezeti egységben, így az irányítást végrehajtó szervezetekben is nagy a fluktuáció, így egy leírt módszer esetében nem kell minden kidolgozói és alkalmazói munkát előröl kezdeni.

Az előzőző fejezetben láthattuk, hogy a NATO és így a Magyar Honvédség előtt álló egyik legnagyobb feladat a hálózat nyújtotta képesség kialakítása, így azt is láthattuk, hogy ez nem csak kifejezetten katonai feladat, ebben részt vesznek majdan különböző kutató bázisok és polgári szervezetek is.

Egyik kiemelt feladatként mutattuk be az egységes vezetési szemlélet kialakításának kérdéskörét. A különböző nemzeteknek és szervezeteknek jelenleg nincs egységes vezetési rendszerük, így egy új megoldás kialakítása során példaként jöhet számításba egy, a polgári életben már bevált, nemzetközi szabványokon alapuló vezetési rendszer. A híradó és informatikai rendszerekben a szakterületektől függően az alábbi szabványokon alapuló rendszereket érdemes vizsgálatok tárgyává tenni [6]:

- MSZ EN ISO 9001 Minőségirányítási rendszerek;
- MSZ EN ISO 14001:2005 Környezetközpontú irányítási rendszerek;
- MSZ ISO/IEC 20000:2007 Informatika. Szolgáltatásirányítás;

- MSZ ISO/IEC 27001:2006 Informatika, biztonságtechnika, az információbiztonság irányítási rendszerei.

A felsorolt szabványok mindegyike a folyamatszemléletű megközelítést, a PDCA modellt alkalmazza előírásaihoz. A folyamatszemléletű megközelítés metodikájának hatékony bemutatására megítélésünk szerint a 9001-s szabvány alkalmas, az alábbiak szerint: *„Ahhoz, hogy egy szervezet eredményesen és hatékonyan tudjon működni, meg kell határoznia és irányítania kell számos, egymással összefüggő folyamatot. Bármely tevékenység, amely erőforrásokat használ, és amelyet úgy irányítanak, hogy bemeneteket kimenetekké alakítson át folyamatnak tekinthető. Az egyik folyamat kimenete gyakran egyben a következő folyamat közvetlen bemenetét is jelenti."* [7].

A minőségirányítási szabványcsalád alkalmazása a közszférában és ezen belül az információs rendszerekben nem új keletű, amelyet bizonyít az Informatikai Tárcaközi Bizottság (ITB) 1996-ban kibocsátott 9-es számú ajánlása. A 9000-es szabványcsalád eredetileg termelő szervezetek számára került kifejlesztésre, azonban a továbbfejlesztések alkalmával megállapításait általánosították annak érdekében, hogy azok mindenfajta szervezetre alkalmazhatók legyenek. Az ITB 9-es ajánlása [8] a minőségirányítási rendszer kialakításának folyamatát három fő fázisra osztja, amelyek:

- Első fázis: A minőségirányítási rendszer meghatározása, ami alapvetően egy hatáselemzés és tényfeltárás elvégzését jelenti, amely meghatározza a szervezet „egészségi állapotát";
- Második fázis: A minőségirányítási rendszer kialakítása, amelynek során költséghatékony „terápiát" alkalmaznak és kiképzik a munkatársakat a „megelőzés technikáira" annak érdekében, hogy a szervezet „állapota" javuljon, vagy legalábbis ne romoljon;
- Harmadik fázis: A minőségirányítási rendszer javítása, amely a folyamatos önjavítást célozza meg a vevőktől, illetve a gazdálkodásból származó haszon növelése érdekében.

Ezt a három fázist az ajánlás összesen további nyolcvanhat feladatra bontja. Természetesen, ha valaki be akar vezetni egy minőségirányítási rendszert nem kötelező követni ezt a felosztást, a számokkal csak a tennivalók mennyiségét szerettük volna bemutatni. A minőségirányítási rendszert csak a rendszerben dolgozók, illetve a rendszert teljesen átvizsgáló szervezetek képesek eredményesen kialakítani.

5. A VIRTAR ÜZEMELTETÉSÉVEL KAPCSOLATOS TEVÉKENYSÉGEK. A HÁLÓZAT FELÜGYELET ÉS A SZÁMÍTÓGÉPES INCIDENSKEZELŐ KÖZPONT FELADATAI

A híradó és informatikai rendszer vezetése magába foglalja a hadműveleti és az üzemeltetést irányító funkciókat is. Az üzemeltetést irányító funkciók két részből kell, hogy álljanak, a hálózat felügyelet, valamint a veszélyjelző és incidenskezelői feladatokból.

5.1. Hálózat felügyelet feladatai

A feladatot jelenleg a MH Támogató Dandár keretében működő hálózat-felügyeleti központ látja el, amelynek a deklarált feladata: *„Az MH zártcélú híradó és informatikai hálózatának központiüzem-felügyelete, menedzselése, a menedzsmentrendszer üzemeltetése, a szerviztevékenység központi irányítása, országos szintű műszaki nyilvántartás vezetése."* [9]. Részleteiben az alábbiakat jelenti:

- Szoftveres és hardveres frissítések végrehajtása;
- A rendszer felügyelete;
- Kapcsolattartás;
- Működőképesség ellenőrzése, hibák javítása;
- Híradó és informatikai támogatás végrehajtása;
- Naplófájlok kezelése;
- Véleményezés, bedolgozás;
- Tudakozó és helpdesk.

5.2. Számítógépes incidenskezelő központ (CIRC) feladatai

Megítélésünk szerint a CIRC feladatait a már bevált gyakorlatokra célszerű építeni. A tervezés során a következő feladatrendszerek kerülhetnek előtérbe:

- Jelzések és figyelmeztetések adása;
- Értesítések a szervezeteknek;
- Biztonsággal kapcsolatos információk terjesztése;
- Incidenskezelés;
- Sérülékenység kezelés;
- Kártékony informatikai termékek kezelése, jelentése a szervezeteknek.

6. A VIRTAR VEZETÉSI SZINTJEI

Kitüntetett kérdésnek tartjuk annak eldöntését, hogy a fentiekben tárgyalt vezetési funkciók mely szinteken kell, hogy megjelenjenek. Véleményünk szerint a békevezetésnek nem szabad különbözőnek lennie a „hadműveleti" vezetéstől, ezért a kérdés tisztázása során az Összhaderőnemi Doktrínát kell elsődlegesen figyelembe venni, amely anyagban megtalálható tézis, hogy a híradó és informatikai rendszerek vezetése érdekében a katonai felső vezetés és a középszintű vezető szerv állít fel és működtet híradó irányító és hálózatfelügyeleti szolgálatokat. Megfogalmazza továbbá, hogy vezetési elemeket ki kell egészíteni az MH CIRC-cel. A CIRC korábban bemutatott feladatai alapján azonban belátható, hogy elegendő egyetlen szinten, a felső vezetés szintjén létrehozni azt, mivel az alsóbb szinteken létrehozni tervezett incidenskezelő központok megítélésünk szerint csak felesleges redundanciát vinnének a rendszerbe.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A vezetési és információs rendszer technikai alrendszerének (VIRTAR) irányítása nem lehet más, nem alkalmazhat más módszereket, mint a Magyar Honvédség általános vezetése, vagyis a VIRTAR irányításának szervesen integrálódnia kell a haderő vezetési struktúrájába. Jelenleg a Magyar Honvédség vezetését a szolgálati elöljárói, illetve a szakmai vezetés jellemzi. A vezetés eszközei a különböző kiadványok. A nyílt formában jelenleg elérhető dokumentumok alapján nehezen látható át a vezetési rendszer elemeit képező dokumentumok (utasítások, szabályzatok, főnökségi kiadványok, doktrínák stb.) struktúrája, az egymáshoz való viszonyuk kiszámíthatatlan. E jelenség problémaforrást generál, mert nehéz az anyagokat a szövetségi rendszer által megkövetelt sémába illeszteni, vagyis adminisztratív területen, a szabályzók kiadásakor is törekednünk kell az interoperabiltiás megvalósítására.

A különböző dokumentumok kidolgozásakor elkötelezetteknek kell lennünk, hogy kifejlesszük, elfogadjuk és megvalósítsunk fogalmakat, doktrínákat, folyamatokat és

mintákat, amelyek alapján elérjük és fenntartsuk az interoperabilitást. Ez a kompatibilitás, felcserélhetőség, azonosság szükséges szintjének létesítését igényli hadműveleti, eljárási, anyagi-technikai és adminisztratív területen is.

A VIRTAR vezetése a szakmai vezetés körébe tartozik. Megállapítható azonban, hogy a három szakterület, úgymint az adatfeldolgozás, az adattovábbítás, illetve az adatbiztonság vezetése nincs egy kézben, a közöttük levő viszonyok jogszabályilag jelenleg nem rendezettek. A VIRTAR szakmai vezetési rendszerét megvizsgálva látható, hogy a többi szakmai vezetési rendszerhez képest fellelhető egy komoly eltérés is, ami nem más, minthogy a szakmai vezetésnek folyamatosan felügyelnie kell egy működő rendszert is.

A VIRTAR irányítási dokumentumrendszerében tovább bonyolítja a helyzetet, hogy az egyetlen érvényben levő szabályzat is elavult. Igaz, annak ellenére, hogy nincs egységes szabályzat a gyakorlati élet kikényszerítette a működőképességet, így mind a VIRTAR, mind annak irányítása is alkalmazható volt, amely tevékenységnek legjobb példája a Magyar Honvédség által végrehajtott missziós feladatok. Ezek nem lehettek volna sikeresek a megfelelő szintű és biztonságos híradó és informatikai támogatás nélkül.

Ennek ellenére meggyőződésünk, hogy szükség van a mindhárom szakterületet átfogó dokumentumrendszer kialakítására. Véleményünk szerint a Magyar Honvédség előtt álló fejlesztési feladatok hálózatközpontú környezetben való alkalmazási képessége megköveteli a VIRTAR korszerű szemléletű vezetését. Bármely vezetési rendszert is alakítunk ki, célszerű azt írásban rögzíteni.

Az Magyar Honvédség előtt álló egyik legnagyobb feladat napjainkban a hálózat nyújtotta képességek kialakítása. Bemutattuk, hogy ez nem csak kifejezetten katonai feladat, ebben részt vállalnak a különböző kutató bázisok és polgári szervezetek is. A különböző nemzeteknek és szervezeteknek jelenleg nem egységes a vezetési rendszerük, az egységesítés eszköze lehet a polgári életben már bevált nemzetközi szabványokon alapuló vezetési rendszer.

Jelen közleményünkben megvizsgáltuk annak lehetőségét, hogy a polgári életben alkalmazott minőségirányítási szabványcsalád alkalmazása mennyire lehetséges erre a feladatra. Megállapítottuk, hogy a 9000-es szabványcsalád eredetileg termelő szervezetek számára került kifejlesztésre, azonban a továbbfejlesztések alkalmával megállapításait általánosították annak érdekében, hogy a szabványban meghatározott követelmények minden szervezetre alkalmazhatók legyenek, azok típusától, méretétől és az általuk előállított termékfajtáktól függetlenül.

A megvalósíthatósági elemzésemet tekintve összességében megállapítható, hogy a VIRTAR irányítási keretrendszerét ki lehet dolgozni a 9000-es szabványcsalád alapján, azonban ez a kidolgozás erőforrásokat igényel, amelyek a felső vezetés képzési költségeiben, a dolgozók kiképzésében, valamint a kidolgozói munkára fordítandó többlet munkaidő igényben rejlenek.

A közleményben bemutattuk, hogy a technikai fejlődés magával hozott olyan negatív változásokat is, amelyek indokolttá teszik a hálózat-felügyelet mellett létrehozni a számítógép veszélyjelző és incidenskezelő központot (CIRC). Bemutattuk továbbá a hálózat-felügyelet és az incidenskezelő központ viszonyrendszerét és áttekintettük mindkettő alrendszer feladatkörét.

A közleményben foglaltakat áttekintve, az abban megfogalmazottakat mérlegelve az alábbi következtetéseket vonjuk le:

- A vizsgálat időszakát tekintve kijelenthető, hogy a VIRTAR három alapvető szakterületét illetően a vezetés egységessége nem valósult meg, a szakterületi viszonyrendszer korrekt rendezése nem teljesült;
- A technológiai fejlődés következtében megváltozó szövetségesi alkalmazási lehetőségek hazánk tekintetében is előre vetítik a számítógép veszélyjelző és incidens központ (CIRC) megszervezésének és működtetésének szükségességét;

- A VIRTAR vezetésének kialakítását célszerű a megfelelő szabványcsaládra, valamint bevált gyakorlatokra alapozva végrehajtani.

FELHASZNÁLT IRODALOM

[1] 1949. évi XX. törvény: A Magyar Köztársaság alkotmánya 40/B § (3) bekezdés

[2] 2004. évi CV. törvény: a honvédelemről és a Magyar Honvédségről 93-94§

[3] ÁLT 27 Magyar Honvédség Összhaderőnemi Doktrína 2. kiadás 2007 68. oldal

[4] 2134/2006. (VII. 27.) Korm. határozat a Magyar Honvédség irányításának és felsőszintű vezetésének rendjéről

[5] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919)

[6] Négyesi Imre: Az önkormányzatok informatikai stratégiája és a Magyar Információs Társadalom Stratégia összefüggései (Hadtudományi szemle on-line, II. évfolyam (2009) 2. szám, 85-92. oldal HU ISSN 2060-0437)

[7] MSZ EN ISO 9001:2000 Minőségirányítási rendszerek 20. oldal

[8] Négyesi Imre: Informatikai rendszerek oktatása a katasztrófavédelmi szakirányon (ZMNE Konferencia előadás, 2010.05.03.)

[9] A HM Támogató Dandár rendeltetése internet letöltés: http://www.hm.gov.hu/honvedseg/magyar_honvedseg_tamogato_dandar

Tóth András – Töreki Ákos
toth.hir.andras@zmne.hu – toreki.akos@zmne.hu

A KRITIKUS INFRASTRUKTÚRÁK ÉS AZOK VÉDELMI LEHETŐSÉGEI

Absztrakt

A szerzők az előzetes tanulmányaikra, valamit a saját tapasztalataikra támaszkodva foglalják össze a kritikus infrastruktúrák körébe tartozó elemeket, illetőleg állást foglalnak az esetleges katasztrófahelyzet megelőzése és elkerülése érdekében végrehajtandó feladatokkal kapcsolatban nemzeti és nemzetközi viszonylatban. Bemutatásra kerül egy információs hálózat, amely alkalmazásával a védelmi tevékenységek jelentős mértékben megkönnyíthetővé válnak.

The writers summarize the critical infrastructures to lean on their earlier study and their own experience, and deal with the activities in national and international circumstances which are necessary to execute to prevent and shun the possible catastrophe. There is shown an information network with which the protection activities become much easier.

Kulcsszavak: *kritikus infrastruktúra, biztonság, védelem, információs hálózat ~ critical infrastructure, security, protection, information network*

1. A KRITIKUS INFRASTRUKTÚRÁK

A NATO Polgár Védelmi Bizottság (NATO CPC) által meghatározottak alapján a kritikus infrastruktúrák azok a létesítmények, szolgáltatások és információs rendszerek, amelyek olyan létfontosságúak a nemzetek számára, hogy működésképtelenné válásuknak vagy megsemmisülésüknek gyengítő hatása lenne a nemzet biztonságára, a nemzetgazdaságra, a közegészségre és közbiztonságra és a kormány hatékony működésére.

Funkciói alapján a kritikus infrastruktúrák lehetővé teszik a nélkülözhetetlen javak előállítását, szállítását és a létfontosságú szolgáltatások folyamatos elérhetőségét (pl. élelmiszer- és vízellátás, közegészségügy, elektromos energiaellátás, áru- és személyszállítás, bank- és pénzügyi rendszerek stb.). Biztosítják az összeköttetést és az együttműködés képességét (kommunikációs és számítógép-hálózatok, mint kritikus információs infrastruktúrák), hozzájárulnak a közbiztonság és az ország külső biztonságának megteremtéséhez (védelmi célú infrastruktúrák).

A veszélyhelyzetek során érintett főbb infrastruktúra elemek a folyamatos kormányzás feltételrendszere; a közlekedés, szállítás (közúti, vasúti, légi, csővezeték, légvezeték); távközlés; vezetékes, vezeték nélküli informatikai hálózat; bankrendszer; energiaellátás; közművesítés; települési lakásállomány; közszolgálati televízió, rádió; helyi média; posta; távhőellátás; gáz- és olajfeldolgozók, tárolók, vezetékrendszerek; háziorvosi szolgálat; szociális gondozói hálózat; ivóvíz- és csatornarendszerek; kommunális hulladékszállítás; élelmiszerellátás, termelés stb.

Kritikus infrastruktúrák esetén három fő kockázattal kell számolni: technológiai rendellenesség (anyagszerkezeti hiba kiváltotta), külső tényező által kiváltott véletlen baleset (természeti katasztrófa), szándékos sérülés okozása (terrortámadás, szabotázs). Ezek a működésben zavart okozhatnak közvetlen (banki hálózat megbénítása gazdasági veszélyhelyzetet idézhet elő) és közvetett módon (távközlési rendszerek megbénítása távvezérelt eszközök feletti ellenőrzés elvesztéséhez vezetnek, ami pedig esetlegesen

katasztrófával járhat). A következmények elemezhetőek a következő kategóriák alapján: kiterjedés, amelyet a kritikus infrastruktúra valamely elemével kapcsolatos veszteséget azon földrajzi terület nagysága alapján számítják ki és osztályozzák, amelyet a veszteség vagy az adott szolgáltatás megszűnése érinthet – pl. nemzetközi, nemzeti, regionális szint. A második a súlyosság, amely a társadalom, a gazdaság és a kormányzat esetében az infrastruktúra meghibásodásából vagy kieséséből fakadó hatás mértékét jelenti. A hatás mértékét a következőképpen lehet értékelni: nincs hatás, minimális, mérsékelt vagy jelentős. Az ezek elleni védelmi tevékenységek célja a zavarokra vagy megsemmisülésére való felkészülés, az ezekkel szembeni védelem, a károsító hatások minimalizálása, azaz a reagálás és a helyreállítás [1].

Ágazat	Alágazat	Felelős
Energia	kőolaj kitermelés, finomítás, feldolgozás, tárolás és elosztás földgáztermelés, feldolgozás, tárolás és elosztás villamosenergia-termelés, továbbítás, elosztás	Nemzeti Fejlesztési és Gazdasági Minisztérium
Infokommunikációs technológiák	információs rendszerek és hálózatok eszköz-, automatikai és ellenőrzési rendszerek Internet infrastruktúra és hozzáférés vezetékes és mobil távközlési szolgáltatások rádiós távközlés és navigáció műholdas távközlés és navigáció műsorszórás postai szolgáltatások kormányzati informatikai, elektronikus hálózatok	Miniszterelnöki Hivatal, Infokommunikációs államtitkárság, Nemzeti Fejlesztési és Gazdasági Minisztérium
Közlekedés	közúti közlekedés vasúti közlekedés légi közlekedés belvízi közlekedés logisztikai központok	Közlekedési, Hírközlési és Energiaügyi Minisztérium
Víz	ivóvíz szolgáltatás vízminőség ellenőrzés szennyvíztisztítás	Országos Katasztrófavédelmi Főigazgatóság, Környezetvédelmi és Vízügyi Minisztérium
Élelmiszer	élelmiszer előállítás élelmiszer-biztonság	Földművelésügyi és Vidékfejlesztési Minisztérium
Egészségügy	kórházi ellátás mentésirányítás egészségügyi tartalékok és vérkészletek magas biztonsági szintű biológiai laboratóriumok egészségbiztosítás	Egészségügyi Minisztérium
Pénzügy	fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek	Pénzügyminisztérium

Ágazat	Alágazat	Felelős
	bank és hitelintézeti biztonság	
Ipar	vegyi anyagok előállítása, tárolása és feldolgozása veszélyes anyagok szállítása, veszélyes hulladékok kezelése és tárolása, nukleáris anyagok előállítása, tárolása, feldolgozása nukleáris kutatóberendezések hadiipari termelés oltóanyag és gyógyszergyártás	Nemzeti Fejlesztési és Gazdasági Minisztérium, Honvédelmi Minisztérium, Önkormányzati és Területfejlesztési Minisztérium, Igazságügyi és Rendészeti Minisztérium
Jogrend - Kormányzat	kormányzati létesítmények, eszközök közigazgatási szolgáltatások igazságszolgáltatás	Igazságügyi és Rendészeti Minisztérium, Önkormányzati és Területfejlesztési Minisztérium
Közbiztonság - Védelem	honvédelmi létesítmények, eszközök, hálózatok rendvédelmi szervek infrastruktúrái	Igazságügyi és Rendészeti Minisztérium, Honvédelmi Minisztérium, Országos Katasztrófavédelmi Főigazgatóság

2. A KRITIKUS INFRASTRUKTÚRA VÉDELME

A Magyar Köztársaság nemzeti biztonsági érdekének tekinti az ország stabilitását, gazdasági, társadalmi és kulturális fejlődését, lehetőségeinek kibontakoztatását, gazdasági, technológiai és emberi erőforrásainak átfogó és gyors ütemű fejlesztését, a fejlett ipari országok szintjéhez közelítését, a fenntartható gazdasági növekedést, állampolgárai biztonságának és jólétének előmozdítását és egy mindezeket sokoldalúan elősegítő biztonsági környezet kialakítását [2].

A védelem érdekében olyan programokat, tevékenységeket kell az államnak, a tulajdonosoknak és az üzemeltetőknek alkalmazni, amelyek biztosítják az esetleges zavarok, szétzúzások megakadályozását, csökkentik a következményeket, valamint általuk a reagálás és a helyreállítás képessége nagymértékben növelhető.

Az Európai Unió célja a védelmi tevékenységek következtében csökkenteni a meghibásodások lehetőségét, elérni, hogy a működési zavarok rövidek, ritkán előfordulóak, a problémák kezelhetőek, földrajzilag lokalizálhatóak legyenek, a lakosságot a lehető legkisebb mértékben érintse. Nagy hangsúlyt fektetnek a gyors és ellenőrzött eljárások kidolgozására. Magyarországon a fő cél, hogy folyamatos, dinamikus rendszert kerüljön létrehozásra, amely a nemzeti kritikus infrastruktúra tulajdonosok, üzemeltetők és a kormányzat együttműködésén alapul. Fejleszteni kívánják ezen eszközök, berendezések, hálózatok működésének megszakadása, vagy kiesése elleni védelemre vonatkozó képességeket az üzemfolytonosság és az ellenálló képesség növelésével, valamint jelzőrendszerek kiépítésével. A kormánynak e célok elérése érdekében keretjogszabályokat kell megalkotnia, egy nemzeti koordinátor szervezetet kell kijelölnie, össze kell állítania egy a kritikus infrastruktúra elemeket tartalmazó dokumentációt, illetve jóvá kell, hogy hagyja az ágazati biztonsági intézkedéseket [3]. A Nemzeti Kritikus Infrastruktúra Védelmi (NKIV) program koordinálja, ellenőrzi és felügyeli a védelemmel kapcsolatos tevékenységeket, valamint biztosítja a veszélyeztetettségi információkat. A központi államigazgatási szervek

dolgozzák ki az ágazati programokat, együttműködnek a tulajdonosokkal és üzemeltetőkkel valamint kockázatkezelési és elemzési programokat készítenek. Hatáskörébe tartozik az Európai Uniós Kritikus Infrastruktúra (EUKI) elemekre történő javaslattétel, védelmi intézkedések és beruházások előkészítése, az információáramlás elősegítése. Az infrastruktúra tulajdonosok, üzemeltetők feladata kockázatkezelési eljárások és a biztonsági beruházások megvalósítása; veszély, sebezhetőségi és egyéb tervezés szempontjából releváns információk továbbítása; üzemeltetői biztonsági terv kidolgozása; illetve felelősek az infrastruktúra védelmének megszervezéséért. Mindenki számára közös feladatok:

- tulajdonosok, kezelők jogainak, kötelezettségeinek jogszabályi rendezése;
- kritikus ágazatok és az ágazati koordináló minisztériumok kijelölése;
- nemzeti riasztási és információs platform működtetése;
- a kritikus infrastruktúrák elemeinek felmérése;
- a biztonsági fejlesztések irányának és a prioritások kijelölése;
- szektorelemzés, ágazati fogalmak, kritériumok kidolgozása;
- védelmi intézkedések, prioritási listák felállítása;
- titkosság biztosítása;
- nemzeti kritikus infrastruktúra védelmi kormányzati konzultációs fórum megteremtése;
- védelem finanszírozása, kutatások, projektek ösztönzése;
- nemzetközi együttműködés;
- közös módszertanok, gyakorlatok kialakítása;
- jogszabály előkészítése, megalkotása;
- figyelmeztető információs hálózat, riasztási rendszer: szinkronban a Critical Infrastructure Warning Information Network (CIWIN)[1] informatikai-távközlési rendszerrel.

3. A LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK FIGYELMEZTETŐ INFORMÁCIÓS HÁLÓZATA

A létfontosságú infrastruktúrák figyelmeztető információs hálózatára (CIWIN) irányuló kezdeményezés a létfontosságú infrastruktúrák védelmére vonatkozó európai program (EPCIP[2]) részét képezi, és különösen az Európai Unió tagállamai közötti információcsere-eljárással és az ezt az eljárást támogató információtechnológiai rendszerrel foglalkozik. A CIWIN létrehozására az EPCIP-ről szóló közlemény (COM (2006) 786 végleges[3]) tett javaslatot, amely meghatározza az uniós létfontosságú infrastruktúrák védelmére vonatkozó horizontális keretrendszert, beleértve a CIWIN-t is magában foglaló EPCIP végrehajtásának megkönnyítésére irányuló intézkedéseket is.

A főbb problémákat a következők jelentették:

- az Európai Unió létfontosságú infrastruktúráira vonatkozóan a védelem módozatai részletesebb vizsgálatának szükségessége;
- a létfontosságú infrastruktúrák tekintetében az Európai Unió tagállamai közötti együttműködés és információcsere javításának szükségessége;
- ugyanannak a tevékenységnek a párhuzamos végrehajtása;
- az érzékeny információk cseréje tekintetében az érdekelt felek elégtelen bizalma és készsége.

1 Létfontosságú infrastruktúrák figyelmeztető információs hálózata
2 European Programme for Critical Infrastructure Protection
3 Az Európai Közösségek Bizottsága: A Bizottság Közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, Brüsszel, 2006.12.12.

A konkrét kérdés, amely uniós szintű fellépést kívánt, a tagállamok hatóságai közötti információcsere megkönnyítése (például a bevált módszerekre vonatkozóan), valamint a létfontosságú infrastruktúrák védelmére (CIP[4]) vonatkozó sürgősségi riasztórendszer használatának lehetővé tétele számukra.

A CIWIN célja a CIP javítása az Európai Unióban, valamint a CIP-re vonatkozó információk tekintetében az uniós szintű koordináció és együttműködés megkönnyítése.

A CIWIN operatív célkitűzései a következők:

- egy olyan információtechnológiai eszköz biztosítása, amely az ennek érdekében együttműködni szándékozó tagállamokat segíti;
- az Európai Unióban a létfontosságú infrastruktúrákra vonatkozó információk keresése tekintetében a gyakran időigényes módszerekkel szemben hatékony és gyors alternatíva megteremtése, azaz a létfontosságú infrastruktúrákkal kapcsolatos valamennyi információ vonatkozásában „egyablakos" rendszer kialakítása;
- annak biztosítása, hogy a megosztott információ biztonságos legyen;
- a tagállamok számára annak lehetővé tétele, hogy közvetlenül tudjanak kommunikálni és az általuk fontosnak ítélt információkat fel tudják tölteni.

Mivel egyes tagállamok a CIWIN által nyújtott funkciók közül csak néhányat kívánnak használni, az egyik fő operatív célkitűzés annak a megoldásnak az azonosítása volt, amely lehetővé tenné a tagállamok számára, hogy a rendszer bizonyos részeihez csatlakozzanak, vagy azoktól távol maradjanak [4].

A CIWIN nem forradalmasítja az Európai Unió biztonságát, és azt csak az EPCIP végrehajtása irányába tett számos lépés egyikének kell tekinteni. A CIWIN a CIP témákra vonatkozó kommunikáció megkönnyítését célzó információtechnológiai eszköz, amely új funkciókat biztosít, például híroldalakat, vitacsoportokat, együttműködő környezeteket, dokumentum- és munkafolyam-kezelési funkciókat, amelyek a mindennapi internet vagy a vállalati intranet részét képezik. A CIWIN-nel való munka számos funkciót figyelembe vesz, miközben biztosított, hogy azok megszüntethetőek legyenek és használatuk törölhető legyen, amennyiben kiderül, hogy nem nyújtanak többletértéket, vagy ha ütköznek a kialakult gyakorlattal.

4. A KRITIKUS INFRASTRUKTÚRA VÉDELEM VIZSGÁLATÁNAK TAPASZTALATAI

Ha a kritikus infrastruktúrák valamilyen beavatkozás következtében működésképtelenné válnak, az súlyos következményekkel járhat az ország gazdaságára, működésére. A 21. században a legtöbb kritikus infrastruktúra a világot behálózó informatikai és kommunikációs rendszerekre épül. A legnagyobb fenyegetettséget számukra a kiberterrorizmus, az információs hadviselés, hackerek, crackerek, gazdasági bűncselekmények, hanyagság, felelőtlenség és természeti katasztrófák jelentik.

A legsúlyosabb problémát elsősorban a villamosenergia-ellátórendszer meghibásodásainak következményei okozzák. A vészhelyzetet a viharos szél, heves esőzés, hirtelen olvadás, áradás okozhatják, amelynek hatásai: az elektromos vezetékek szakadásai, a közműrendszereket alámossa és elönti a víz, akadozó víz-, távhőszolgáltatás, hírközlés és a szállítás, a lakosság alapellátásának hiánya, a veszélyes anyagok tárolásának kockázata, a fertőzésveszély. Egy másik jelentős problémát az informatikai és kommunikációs rendszerek kiesése jelentheti, amely már önmagában is katasztrófahelyzetet idézhet elő, mivel a különböző infrastruktúrák, eszközök és szolgáltatások túlnyomó többségének működése

4 Critical Infrastructure Protection

ezeken a rendszereken alapszik. Az infokommunikációs rendszerek nem csak a fizikai veszélyeknek vannak kitéve, hanem más, a kibertérből érkező támadásokkal szemben is nehezen védhetőek, e rendszerek támadásával – azaz a kritikus információs infrastruktúrák működésének időleges vagy teljes működésképtelenségével – az infrastruktúráink nagy része megbénítható [5].

A védelmi tevékenységekben résztvevő szervezetek fő feladatai a kritikus infrastruktúra elemeinek folyamatos vizsgálata, a működéshez szükséges feltételek kidolgozásában való közreműködés, az önkormányzatok és a lakosság felkészítése az esetlegesen bekövetkező kritikus helyzetek gyors és hatékony kezelésére, az ilyen helyzetben alkalmazandó rendszabályokra, illetve a szükséges teendőkre. A kritikus infrastruktúra védelem jövőbeni feladatai a gazdaság átalakítása, a katasztrófa-érzékeny tevékenységek háttérbe szorítása, az anyagi környezet átalakítása, idomítása a megváltozó körülményekhez, biztosítás kötése vagy más kockázatmegosztó technikák alkalmazása [6].

HIVATKOZÁSOK

[1] Halász Péter mk. alezredes: A védelmi infrastruktúra főbb alkotó elemeinek kölcsönhatása, továbbá közös fejlesztésük lehetőségei, doktori (PhD értekezés), ZMNE, Budapest, 2006.

[2] 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról, Határozatok Tára, 2004. évi 15. szám

[3] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, Határozatok Tára, 2008. évi 31. szám

[4] Az Európai Közösségek Bizottsága: A Bizottság Közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, Brüsszel, 2006.12.12.

[5] Muha Lajos: A Magyar Köztársaság kritikus infrastruktúráinak védelme, doktori (PhD értekezés), ZMNE, Budapest, 2007.

[6] Nagy Rudolf mk. pv. alezredes: A kritikus infrastruktúra védelme és katasztrófavédelmi aspektusai a terrorizmus tükrében, Kard és Toll, Budapest, ISSN 1587-558X, 2006/3. szám, 56-64. oldal, 2006.

Töreki Ákos
toreki.akos@zmne.hu

AZ IP ALAPÚ HÁLÓZATOK KIALAKULÁSA, A HÁLÓZATOK INTEGRÁCIÓJÁNAK FOLYAMATA

Absztrakt

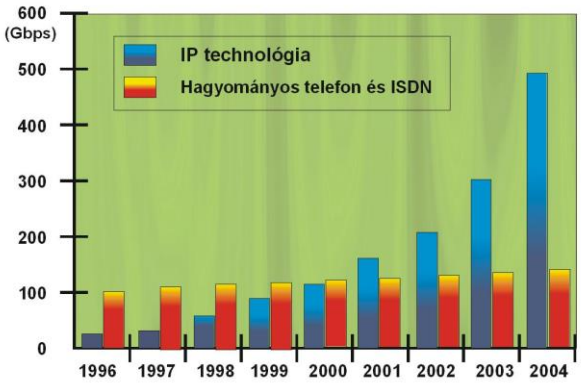
A cikk az IP alakú hálózatok kialakulásának és fejlődésének fő mozzanatait mutatja be. Leírja a csomagkapcsolt technológia szerepét a távközlési hálózatok integrációja területén. Ezáltal rövid történeti áttekintést nyújt napjaink „multiservice" hálózatainak létrejöttéig.

This article describes the main phases of the IP networks' invention and development. It submits the role of the packet switched technology about the integration of the communication networks, hereby gives a short historic summary till the evolution of present days' „multiservice" communication networks.

Kulcsszavak: *IP alapú hálózat, Internet, kommunikáció ~ IP network, Internet, communication*

BEVEZETÉS

Az átviteli technológiák közül napjainkban a csomagkapcsolt Internet Protokoll a legelterjedtebb. Az IP alapú hálózatok nemcsak felvették a versenyt a hagyományos távbeszélő hálózatokkal, hanem túl is szárnyalták azok forgalmát (1. ábra).



1. ábra: A hagyományos távközlés és ISDN típusú kommunikáció adatsebessége az IP technológiához hasonlítva
Forrás: NTT

Az adat-, hang- és videojel átvitelre egyaránt alkalmas csomagkapcsolt hálózatok szolgáltatásainak sokszínűségét és a szolgáltatások minőségi változásait tekintve nem meglepő, hogy a jövő távközlési irányvonalát az IP hálózatok kialakítása fogja képezni. Ezen hálózatok kiépítése és működtetése, valamint menedzselése is gazdaságosabban oldható meg, mint a vonalkapcsolt megfelelőik esetében.

Az első, tisztán csomagkapcsolt hálózatnak az USA-ban kiépített NSFNET-et tekintik, amely továbbfejlődésével létrejött a mai Internet.

1. A TCP/IP HÁLÓZATOK KIALAKULÁSA

A nagy horderejű technikai, technológiai vívmányok nem kis részét köszönhetjük különböző katonai kutató és fejlesztő (röviden K+F) programoknak. Aki ezzel tisztában van, az talán nem lepődik meg azon sem, hogy a sokunk által használt Internet kialakulásában is fontos szerep jutott a katonai szférának.

Az 1960-as években az Amerikai Egyesült Államok Védelmi Minisztériumának (Department of Defense, röviden DoD) Kutatási Hivatala (Advanced Research Project Agency, röviden ARPA) belekezdett egy kettős célú projektbe. Elsődlegesen számítógépeket akartak hagyományos kapcsolástechnikai eszközökkel (modemmel, telefonvonalakon keresztül) hálózatba kapcsolni oly módon, hogy egy vonalat ne csak egy felhasználó használhasson.

A Pentagon számítógép hálózatok kiépítésével kapcsolatos terveiből, valamint az akkori hidegháborús állapotokból vezethető le a kutatás másik, ugyancsak nem kevésbé fontos célja: Mivel a Pentagon katonai, valamint kulcsfontosságú fejlesztési központok összekötésére alkalmas rendszert akart létrehozni a hidegháborús fenyegetettség időszakában, így fontos szempont volt a rendszer magas fokú túlélőképessége is például egy rakétacsapás vagy bombázás során.

Ekkor született meg a csomagkapcsolt hálózat (angolul packet-swiched network) ötlete, amelynek tömör lényege az, hogy a továbbítandó információ csomagokra darabolva kerül a hálózatra, amely csomagok akár eltérő utakon is haladhatnak majd miután eljutnak a címzetthez, újra felépíthető belőlük a továbbított információ. Mivel a csomagok a főinformáción kívül a csomagok sorrendjére és a címzettre vonatkozó információval is rendelkeznek, így egy (vagy több) csomópont kiesése (megsemmisülése), vagy egy vonal szakadása esetén más csomópontok, vonalak érintésével, automatikus átirányítással is továbbítható az üzenet.

Ez azt is jelenti, hogy a hálózat túlélőképessége magasabb lesz, mivel decentralizált, vagyis nem rendelkezik olyan központi bázissal, amely kiesése működésképtelenné tenné az egész rendszert.

2. AZ INTERNET ELŐFUTÁRA, AZ ARPANET

1969. decemberében a kutatás-fejlesztés eredményeként életre keltettek egy kísérleti hálózatot, amely kezdetben mindössze négy csomóponttal rendelkezett. Ez volt az ARPANET első struktúrája. A csomópontok a következő intézményekben voltak:

- University California at Los Angeles (UCLA);
- University California at Santa Barbara (UCSB);
- Stanford Research Institute (SRI);
- University of Utah (UTAH).

A négy intézet összekapcsolását nehezítette az, hogy mindegyikben különböző típusú, egymással nem kompatibilis számítógépek voltak.

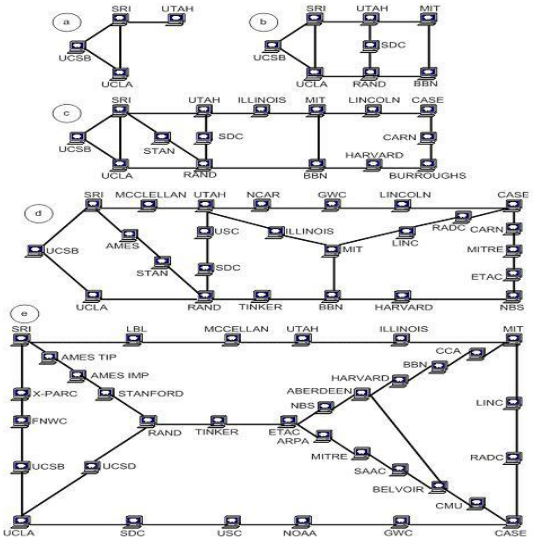
Az ARPANET négy csomópontja 1971-ben tizenötre, 1972-ben már harminchétre emelkedett és lassan lefedte az egész országot.

Az így létrehozott hálózat csomóponti gépeihez esetenként több hoszt[1] is csatlakozott és egy adott hoszt elérhetett más csomóponti gépeket is, így kiküszöbölték a csomóponti gépek meghibásodásából származó problémákat. Fejlesztések folytak a hosztok és csomóponti gépek közötti távolság megnövelésére is, amely azt tette lehetővé, hogy a hosztokat az alhálózattól távolabb is elhelyezhették.

A későbbiekben az ARPANET nemcsak a telefonhálózatot használta átviteli közegként. Az ARPA kutatásokat végzett, hogy műholdas és mobil csomagkapcsolású rádiós hálózatokat felhasználva szélesítsék az ARPANET rejtette lehetőségeket.

A csomagkapcsolt adattovábbítás a katonai felhasználáson kívül további kutatási célokat szolgált, továbbá egyes egyetemek, kormányzati laboratóriumok és katonai bázisok felhasználói elektronikus levelezésre, file-ok küldésére is használták.

1983-ban a hálózatot két elkülönített részre bontották. Az egyik fele megmaradt ARPANET néven további kutatásokra, kísérletezésekre, a másik rész pedig kizárólag katonai felhasználásra, MILNET néven működött tovább. A két hálózat össze volt kötve, de a kapcsolat bármikor megszakítható volt. (Az ARPANET fejlődését a 2. ábra mutatja.)



2. ábra: Az ARPANET fejlődése: (a)1969. december, (b)1970. július, (c)1971. március, (d)1972. április, (e)1972. szeptember
Forrás: Tanenbaum

3. AZ NSFNET

Még az ARPANET ki sem nőtte magát, mikor már az egyesült államokbeli Nemzeti Kutatási Alap (National Science Foundation, röviden NSF) felismerte a benne rejlő lehetőségeket. Mivel ez a típusú hálózat lehetővé tette, hogy a kutatók országszerte hozzáférhessenek bármiféle adathoz, valamint közös projekteken dolgozhatnak a földrajzi távolságok „egy gombnyomásra történő” áthidalásával, így óriási hatással bírt a tudományos kutatásokra.

1984-ben az NSF nekilátott egy olyan nagy sebességű hálózat kifejlesztésének, amelynek struktúrája az ARPANET-en alapult, viszont egy lényeges –nem technológiai– dologban eltért attól. A különbség abból adódott, hogy az NSF hálózatát úgy tervezték, hogy minden

1 Hoszt: olyan számítógép, amelyik egy hálózathoz csatlakozik függetlenül attól, hogy rajta keresztül hány felhasználó használja a szolgáltatást

egyetemi kutatócsoport számára nyitott legyen, ellenben az ARPANET-tel, amely elérhetőségét szerződéshez kötötték.

1985. és 1986. között az NSF egy gerinchálózatot épített ki, amellyel összekapcsolta hat szuperszámítógép központját. A hat központ:

- San Diego;
- Boulder;
- Champaign;
- Pittsburg;
- Ithaca;
- Princeton.

A hat központot 56 kb/s-os bérelt telefonvonallal kötötték össze, mint ahogy azt az ARPANET-nél is tették.

Az NSF ezen hálózatának gerinchálózati funkciója volt, vagyis a különböző területeken kialakított regionális hálózatokat kapcsolta össze és csatlakoztatta az ARPANET-re. Ezáltal több egyetem, kutatóintézet és más intézmények számára elérhetővé váltak a szuperszámítógépek, vagyis azok adatbázisai. Ezt a hálózatot nevezték NSFNET-nek, amely magába foglalta a gerinchálózatot és a regionális hálózatokat.

Rövid időn belül magas számban csatlakoztak az alhálózatok az NSFNET-hez, ezért az NSF úgy döntött, hogy megtervez egy kettes számú hálózatot is, amelyhez már 448 kb/s-os optikai kábeleket bérelt. Az ugrásszerűen megnőtt kliensek miatt azonban hamarosan ez is kevésnek bizonyult. Az újabb fejlesztések eredményeként 1990-re a gerinc kapacitása elérte az 1,5 Mb/s-os sebességet.

Mivel a kormány támogatása véges volt és kereskedelmi szervezetek is kapcsolódni kívántak az NSFNET-hez, ezért az NFS és a második generációs hálózat kiépítésében részt vállaló szervek úgy döntöttek, hogy életre keltenek egy non-profit szervezetet, amely elősegíti a hálózatok kereskedelmi forgalomba helyezését. Ez a szervezet az ANS (Advanced Network Services) lett.

Az ANS 1990-ben átvette az NSFNET-et és a vonalak sebességét 45 Mb/s-ra növelte. Az NSFNET rövid időn belül az USA domináns gerinchálózata lett.

Az NSFNET-hez hasonló hálózatok más országok is létrejöttek. Ilyen például az európai EuropaNet, vagy az EBONE. Míg az EuropaNet kutatóintézeteket köt össze, addig az EBONE kereskedelmi célú hálózat. Ezen hálózatok európai nagyvárosokat kapcsolnak össze. NSF regionális hálózatra hasonlító hálózatot azonban mindegyik európai országban lehet találni.

4. AZ INTERNET TÖRTÉNETE

A ’80-as évek vége felé a különböző országokban kiépült gerinchálózatok igyekeztek az NSFNET-hez kapcsolódni, de emellett gyakran közvetlen kapcsolatot is építettek egymás között. Ezen kapcsolódásoknak volt köszönhető a hálózat és persze a felhasználók számának rendkívüli mértékű növekedése, amely az Internetwork system, röviden az Internet kialakulásához vezetett.

Az Internet felhasználók kezdetben oktatási és kormányzati intézmények, ipari kutatóintézetek voltak. Ezt a helyzetet leginkább a World Wide Web (röviden www), azaz a Világháló megjelenése formálta át és tette lehetővé bárki számára az Internet használatát. Mindennek köszönhetően a ’90-es évek elejétől felgyorsultak az események. 1990-ben megjelent az első, kezdetleges böngésző (Mosaic), majd négy ével később a Netscape, amely segítségével PC-tulajdonosok millióinak adatott meg a lehetőség, hogy hozzáférhessenek és használhassák az Internetet.

A robbanásszerű fejlődés új módszereket hozott az Internet használatával kapcsolatban. 1992-ben megalakult egy non profit jellegű szervezet, az Internet Society (röviden ISOC), amely az Internet új formában történő felhasználását segítette, majd az Internet legfontosabb szervező, összefogó ereje lett. Az ISOC fő célja az Internet alapon történő információcsere összehangolása, a technológia fejlesztése, valamint az ezzel kapcsolatos ajánlások kidolgozása.

Az ISOC felkért egy szakemberekből álló bizottságot, az Internet Activities Board-ot (röviden IAB) a következő feladatok ellátására:

- Állásfoglalás alapvető stratégiai kérdésekben;
- Szabványosítást igénylő kérdések meghatározása;
- Szabványok elfogadása;
- Internet címzési rendszer karbantartása.

Az Internet világszerte elterjedt hálózata az IAB-n, azaz a protokollokat és a címek kiosztását ellenőrző bizottságon kívül semmiféle központi menedzsmenttel nem rendelkezik.

1990-re az Internet már közel 3000 hálózatot és 200 000 számítógépet foglalt magába. 1992-ben a hosztok száma elérte az egymilliót. 1995-re számos gerinchálózat, több száz középszintű (azaz regionális) hálózat, több tízezer LAN, több millió hoszt és több tízmillió felhasználó alkotja az Internetet.

1995-ben már 42 millió Internet felhasználót számláltak, 2000-re ez a szám megtízszereződött és napjainkban újabb ugrásszerű emelkedés tapasztalható, ami a mobil hozzáférést biztosító eszközök elterjedésének köszönhető.

Az ember szinte fel sem tudja sorolni, hogy mi mindenre használják manapság az Internetet. A sokféle alkalmazás mögött Tanenbaum szerint négy fő alkalmazási terület áll. Ezek a következők:

- Elektronikus levél (1);
- Hírek (2);
- Távoli bejelentkezés (3);
- File-transzfer (4).

1. Az elektronikus levelezés még az ARPANET idején vált lehetővé. Azóta a levelek szerkesztése, elküldése és fogadása is sokat változott, de az alaprendeltetés a régi maradt. Az E-mail egyre nagyobb népszerűségnek örvend.

2. Hírek. A hírcsoportok olyan speciális fórumok, amelyek az azonos érdeklődésű emberek számára lehetővé teszik véleményük kicserélését. Több ezer hírcsoport létezik műszaki és nem műszaki témákban. Ilyen például a számítástechnika, a tudományok, a szórakozás vagy a politika.

3. A távoli bejelentkezés lényege az, hogy az Interneten keresztül az ehhez szükséges programok (pl.:Telnet, Rlogin) segítségével bejelentkezhetünk olyan számítógépekre, amelyhez hozzáférési jogunk van.

4. A file-transzfer az Internetre csatlakozott számítógépek közötti file-ok másolását jelenti. A felhasználók számára így rengeteg információ válik elérhetővé.

A rengeteg hálózatot, több millió felhasználót magába foglaló Internet a XXI. századra szerves része, alappillére lett az információs társadalomnak.

5. A HÁLÓZATOK INTEGRÁCIÓJA

A távközlés a közelmúltban alapvető változásokon ment át és napjainkban is formálódik. A törekvések elsősorban arra irányulnak, hogy olyan hálózatokat hozzanak létre, amelyek

alkalmasak hang-, adat- és videójelek továbbítására egyaránt akár vezeték nélküli eszközök között is.

A távközlési szolgáltatóknak is érdeke mindez, hiszen számukra is előnyösebb egyetlen hálózat kiépítése, üzemeltetése, fejlesztése, mint mondjuk külön vonalkapcsolt telefon hálózat, csomagkapcsolt adathálózat és emellett még egy mobil hálózat fenntartása is.

A hálózatok fejlődését három szakaszra bonthatjuk, ezek a következők:

1. szakasz: Az 1980-as évek elején elterjedtek a hangszolgáltatásokat nyújtó hálózatok. A nagy állami postai és telekommunikációs vállalatok mellett megjelentek a saját tulajdonú alternatív szolgáltatók is. A szolgáltatók számának növekedése miatt kialakult versenyhelyzet a kommunikációs technológia, és az azokat megvalósító termékek gyors fejlődéséhez vezetett. Megjelentek az első digitális központok, telefonüzenet-rögzítő rendszerek.

2. szakasz: Az 1990-es évek közepére az adathálózatok elterjedése világméretű méreteket öltött. Az asztali számítógépek számának rohamos növekedése magával hozta a gépek hálózatba kapcsolásának igényét, ami a lokális hálózatok megjelenéséhez vezetett. Fontos szerephez jutottak a LAN[2]-ok összekapcsolására szolgáló magán-, és közcélú adathálózatok.

3. szakasz: Az új fejezetet az 1990-es évek vége hozta, amikor az eddig különböző funkciót ellátó, egymástól független hálózati infrastruktúrát igénybevevő hang-, és adatszolgáltatás egyetlen közös „multiservice" hálózaton történő működtetése lehetővé vált.

ÖSSZEGZÉS

A konvergens hálózatok "egyesítő ereje" az Internet Protokollon alapuló csomagkapcsolt technológia lett. Az új, egységes hálózat így egyetlen technológiával képes hang, adat és video forgalom továbbítására.

Az ilyen hálózat előnyei közé tartozik a nagyobb teljesítmény, a hálózat módosítása, továbbfejlesztése, irányítása során tapasztalható nagyobb rugalmasság, az új alkalmazások és hálózati szolgáltatások gyorsabb használatbavétele. Továbbá kisebb a beruházási, továbbfejlesztési, karbantartási költség, mert elég egyetlen, multifunkcionális infrastruktúrát beszerezni, kevesebb szakemberrel, kisebb tartalék erőforrással (pl.: alkatrészkészlettel) üzemeltetni. A több különböző célú hálózati infrastruktúrára szánt beruházási költségkeretből egy nagyobb teljesítményű, jobban terhelhető „multiservice" hálózatot lehet létrehozni.

A hang-, adat-és videoforgalom továbbítása más-más terheléssel bír a hálózatra. Egy közös infrastruktúrán való működtetésük azzal az előnnyel is jár, hogy együtt egyenletesebben terhelik, gazdaságosabban használják ki a közös infrastruktúrát.

FELHASZNÁLT IRODALOM

- Géher Károly: Híradás technika, Műszaki könyvkiadó, Budapest, 2000
  ISBN 963 16 0173 0
- Andrew S. Tanenbaum: Számítógép-hálózatok, Panem Prentice Hall, Budapest, 1999
  ISBN 963 545 213 6
- Móricz Attila: Az internet újdonságai, LSI Oktatóközpont, Budapest, 1998
  ISBN 963 577 225 4
- Az internet története
  (http://izzo.inf.elte.hu/~hehe/ve2002/halozat/tori.htm)

2 LAN: Local Area Network, azaz helyi, lokális hálózat

- NIIF VoIP pilot projekt (http://www.iif.hu/index.php?headline=alkalmaz&text=iptel.html&nomenu=1)
- Szabó Zoltán: Konvergencia a távközlési fajták között (http://informatika.bke.hu/root/Project/telepiac.nfs)

Papp Zoltán
pappz.szeged@gmail.com

VIRTUÁLIS MAGÁNHÁLÓZATI KAPCSOLATOK

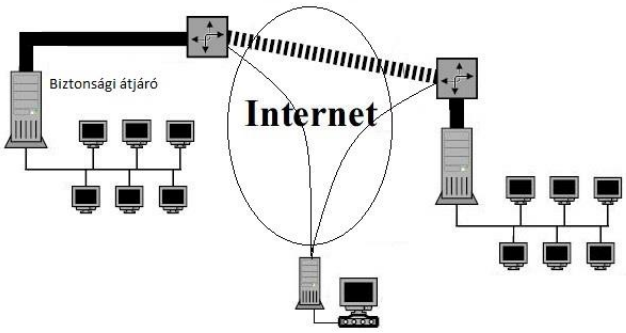
Absztrakt

Az Internet egyre nagyobb szerepet játszik az élet minden területén, így a rendvédelmi szervek kommunikációjában is. A rendészeti tartalmú kommunikáció során pedig kulcsfontosságú a hálózat biztonsága. A bemutatandó technológia olyan megbízható megoldást kínál, amellyel földrajzi korlátok nélkül megoldható, hogy a szervezeti egységek az Interneten keresztül biztonságosan, ugyanakkor teljes körűen hozzáférhessenek egymás hálózataihoz, alrendszereihez.

Internet plays an increasingly important role in all areas of life, including the communication of law enforcement organisations. Network security is of key importance in terms of communication with law enforcement content. The technology presented here offers a reliable solution that enables organisational units to get a secure yet complete access to each other's networks and subsystems via Internet without any geographical limitations.

Kulcsszavak: *virtuális magánhálózat, hálózati biztonság, Internet, kommunikáció ~ virtual privat network, network security, Internet, communication*

A virtuális magánhálózat (Virtual Private Network - VPN) olyan technológiák összessége, amelyek azt biztosítják, hogy az egymástól távol eső szervezeti egységek számítógépei, kommunikációs eszközei egy kizárólag saját célra kialakított és fenntartott, továbbiakban privát hálózatokként biztonságosan kommunikálhassanak egymással, valamilyen publikus hálózaton keresztül – ami napjainkban tipikusan az Internet – amely egyébként nem biztonságos.



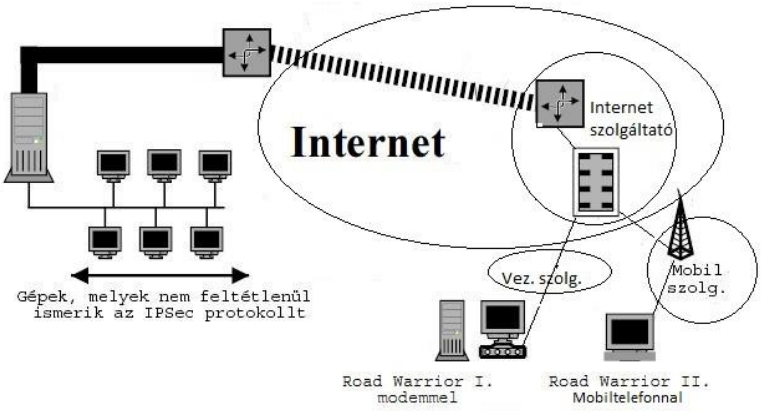
1. ábra

A közvetlen kapcsolat emulálása érdekében az adatokhoz egy fejléc fűződik, ami az adatcsomagnak a végpont megosztott vagy nyilvános hálózaton keresztül történő eléréséhez szükséges útvonalára vonatkozó információkat tartalmazza. Magánkapcsolat emulálásánál biztonsági szempontok miatt az adatok titkosítva vannak. A megosztott vagy nyilvános hálózaton elfogott csomagok a titkosító kulcsok nélkül olvashatatlanok.

A biztonsági megoldások gyártónként eltérőek, de szinte mindegyik VPN az adatátvitel során alkalmaz valamiféle kódolást. A szolgáltatást a gép vagy felhasználó csak egy erős azonosítási mechanizmus sikeressége után veheti igénybe. Fontos követelmény, hogy az alkalmazott megoldásnak el kell rejtenie a privát hálózat belső felépítését, topológiáját a potenciális külső támadóktól.

Egy VPN kialakítása során minden egyes összekapcsolni kívánt hálózatrész és a publikus hálózat közé biztonsági átjárókat helyeznek el. Az átjárók titkosítják a csomagokat, melyek elhagyják a privát hálózatot és dekódolják a publikus hálózatból érkező csomagokat, ezzel titkosított csatornát alakítva ki a publikus hálózaton. Ha az alkalmazott kriptográfiai eljárás elég erős, a megvalósítás elég körültekintő és az adminisztrációt hozzáértően konfigurálják, akkor a kommunikáló felek bízhatnak ebben a csatornában. Innentől kezdve az összekapcsolt hálózatrészek úgy viselkednek, mintha egyetlen hatalmas privát hálózatot képeznének.

A VPN alapértelmezésben bizonyos hálózatrészek összekapcsolását jelenti. Ennek speciális esete, amikor nem, vagy nem csak hálózatrészeket kapcsolunk össze, hanem hálózatrészt, vagy részeket egy konkrét számítógéppel (un. Road Warrior). Ez például lehet akár egy utcán lévő rendőrjárőr, aki mozgó kommunikációs eszközről (például egy laptopról) kapcsolódik a privát hálózatba, hogy onnan munkájához szükséges információkat kérjen le. Adminisztratív szempontból ez megegyezik azzal az esettel, amikor valaki otthoni gépéről próbál bejutni az irodai hálózatba úgy, hogy nem rendelkezik fix IP címmel.



2. ábra

A legtöbb hardware alapú megoldás tulajdonképpen olyan router-ek alkalmazását jelenti, amelyek képesek az adatforgalom titkosítására. Használatuk egyszerű, mivel ez a megoldás áll a legközelebb a 'plug and play' titkosítás megvalósításához. A legmagasabb fokú hálózati áteresztőképességet nyújtják az összes többi megoldással szemben, hiszen nem emésztenek fel fölösleges erőforrásokat plusz operációs rendszer és segédalkalmazások kiszolgálására. Mindezen jó tulajdonságaik ellenére korántsem olyan rugalmasak, mint például a software alapú megoldások, éppen ezért a legjobb hardware alapú VPN rendszerek a hozzáférés vezérlés egy részét átengedik, vagy megosztják más korlátozó eszközökkel, mint amilyen a tűzfal.

A tűzfal alapú megoldások kihasználják a tűzfal biztonsági mechanizmus előnyeit, mint például a hozzáférés korlátozását bizonyos hálózatrészek között, a címfordítást, megfelelő azonosítási mechanizmusokat, kiterjedt logolást, valós idejű riasztást. A VPN szerverek

általában a tűzfalakhoz hasonlóan lecsupaszított kiszolgálók, amiken lehetőség szerint semmilyen más alkalmazás nem fut, csak a célhoz szükséges eszközök, a minél kisebb támadási felület mutatása érdekében. Fontos figyelembe venni a VPN teljesítményre gyakorolt csökkentő hatását (főként egy meglévő, amúgy is terhelt tűzfalon veszélyes lehet), habár a legtöbb gyártó itt is célhardver elemeket kínál az általános processzorokon nagy teljesítményt igénylő alkalmazásokhoz, mint amilyen maga a titkosítás.

A software alapú megoldások abban az esetben ideálisak, ha a VPN egy-egy határvonala más-más szervezet, vagy szervezeti egység tulajdonában van, vagy abban az esetben, ha ugyanaz a szervezet, de eltérő a használt eszközök típusa a szervezeten belül. A VPN menedzselésére a legrugalmasabb megoldásokat a szoftverek nyújtják. A legtöbb ilyen programcsomag lehetőséget ad a csomagok címzés, vagy protokoll szerinti tunneling-jére (a csomagok újracsomagolódnak egy PPP szekvenciába és így jutnak el a célhoz, ahol a fogadó visszabontja), ellentétben a hardware alapú megoldásokkal, amelyek általában a protokollra való tekintet nélkül minden forgalmat tunelleznek. Ez a tulajdonság hasznos lehet abban az esetben, ha a távoli gépeknek kétféle minőségű adattal kell dolgozniuk, olyanokkal amelyeket a VPN-en keresztül kell küldeniük (pl. adatbázis bejegyzések a vezetőknek) és olyanokkal, amelyeket nem (web böngészés). Előny még, hogy jól skálázható, hátrány viszont, hogy több háttértudás szükséges a beállításához, mint amilyen a kiszolgáló operációs rendszer széles körű ismerete.

A VPN megvalósítására több módszer létezik, melyek közül különös hangsúlyt fektetnek az IPSec-re, mivel manapság ez a leginkább elterjedt és elfogadott módja egy ilyen feladat megoldásának. Ezt a protokollcsomagot az IETF (Internet Engineering Task Force) dolgozta ki, az egyes protokollok definícióit RFC-kben rögzítették. Az IPSec hálózati szinten nyújt lehetőséget arra, hogy a kommunikációban résztvevők hitelesen azonosítsák egymást és kódolják az egymás közt zajló adatforgalmat.

Az IPSec két szinten is végez hitelesítést:

- A kapcsolat felépítése során biztosítja, hogy a résztvevő felek közvetlenül azzal veszik fel a kapcsolatot, akivel szeretnék;
- A felépült kapcsolatot csomagok szintjén is ellenőrzi, hogy a kommunikációba ne avatkozhasson bele nemkívánatos résztvevő.

Az IPSec kódolás hibrid kulcsú titkosítást használ, így mind a szimmetrikus, mind az aszimmetrikus titkosítást alkalmazza.

A normál IPv4 csomagoknál már megszokott payload és header részeket, amelyeket jól ismert támadási módszerek során módosítanak (például spoofing), IPSec alkalmazása esetén digitálisan aláír a feladó és ezt az aláírást az Authentication Header-be helyez el (AH), ezzel bizonyítva azok hitelességét. Az IPSec Encapsulation Security Payload (ESP), pedig az adatok integritását és bizalmasságát biztosítja oly módon, hogy vagy az eredeti payloaddal és vagy headerrel, vagy egy titkos hash-sel kombinálja az eredeti csomagot. Az Internet Key Exchange (IKE), pedig a kapcsolat paramétereinek megvitatására és a használt kulcsok cseréjére ad lehetőséget.

A magasabb szintű szolgáltatások, mint amilyen például a PGP (Pretty Good Privacy, egy számítógépes program, ami titkosításra és hitelesítésre egyaránt használható) csak egy konkrét protokollt képesek védeni, míg az alacsonyabb szintűek, csak egy adott fizikai médiumot. Ezzel ellentétben az IPSec bármilyen protokollt képes védeni, amely IP fölött fut,

és bármely hosztot, amelyen IP fut. Képes védeni a vegyesen használt alkalmazás-protokollokat is, vegyesen alkalmazott hosztokon, amely az Interneten mindennapos.

Az IPSec képes néhány olyan háttér-szolgáltatást nyújtani, amelynek nincs érzékelhető hatása a felhasználókra. Ellentétben például a PGP-vel, amelyhez a felhasználónak meghatározott lépéseket kell tenni a használat során. A felhasználónak adott esetben nem is kell tudnia, hogy IPSec rendszert vesz igénybe. Annak ellenére, hogy az IPSec nem nyújt email titkosítási funkciót, képes titkosítani az email-t. A gyakorlatban ez úgy valósul meg, hogy ha a támadó a publikus hálózatból tekint a forgalomra, nem tudja elolvasni a levelet. Ebben a szituációban az IPSec ugyanúgy megakadályozta az illetéktelen hozzáférést, mintha PGP-vel lett volna titkosítva a levél.

Az előny ott jelentkezik, hogy ez nem csak az email-ekre igaz, hanem minden IP felett folyó kommunikációra. Az egyetlen, ami egyelőre nem támogatott a protokollban – habár már tervbe van véve – az úgynevezett IP Multicast jellegű kommunikáció védelme.

IPSec átjárók bárhol kialakíthatóak, ahol szükséges:

- A szervezet dönthet úgy, hogy a LAN és az Internet között elhelyezkedő tűzfalon létesít ilyen szolgáltatást. Ezzel a megoldással több szervezeti egységet kapcsolhatnak össze a külvilágtól védetten;
- Egy másik esetben a szervezet úgy dönthet, hogy a szervezeti egységeket összekötő gerinchálózatát védi ezzel a mechanizmussal. Így az üzenetek mindenkitől védettek, csak a küldő és fogadó részleg látja őket;
- Más talán nem az információ titkosításában látja a fő célt, hanem abban, hogy korlátozza a szolgáltatásokhoz és erőforrásokhoz való hozzáférést. Ekkor az IPSec csomaghitelesítést (packet authentication) a hozzáférés vezérlési mechanizmus (access control mechanism) részeként lehet alkalmazni, akár titkosítva, vagy anélkül;
- Igény szerint minden gépre telepíthető IPSec átjáró, ehhez természetesen minden gépen szükséges megfelelő feldolgozó kapacitás megléte. Így minden gép kommunikációjára igaz, hogy csak a forrás és a cél látja azt;
- A fenti lehetőségek tetszés szerint kombinálhatóak.

Azonban ha a biztonsági átjárók nincsenek megfelelően védve a rendszer nem képes megvédeni magát. Ez a protokoll nem ismeri a felhasználó azonosító (user ID) fogalmát, így nem minden biztonságpolitika valósítható meg kizárólag ezzel a technikával. Ha arra van szükség, hogy egy adatbázishoz való hozzáférést bizonyos felhasználókra korlátozzunk, akkor egy másik mechanizmust kell alkalmazni. Ezzel együtt alkalmazhatjuk az IPSec-et is arra, hogy csak bizonyos gépekről legyen elérhető a szolgáltatás és arra, hogy a gépek között a kommunikáció védett legyen, de itt az IPSec feladata véget ér, a további feladatokat más eszközökkel kell biztosítani.

A privát hálózatban elhelyezkedő forrásgéptől a biztonsági átjáróig, illetve a biztonsági átjárótól a másik privát hálózatban lévő célgépig alapértelmezésben semmi sem biztosítja az adatok sértetlenségét. Például ha azt szeretnénk, hogy egy bizalmas tartalmú email-t kizárólag a címzett olvasson el, akkor mindenképpen PGP-t kell alkalmaznunk. Az IPSec nem gátolja meg a forgalomelemzést, aminek során sok információ származtatható a forgalomból anélkül, hogy ismernénk a kódolást, vagy értenénk az üzeneteket. Például a titkosított csomagok fejlécei kódolatlanok, úgy mint a forrás- és célátjáró címe, a csomagok mérete, stb. amelyeket összegyűjtve és elemezve sok mindenre lehet következtetni. További hátrány, hogy az IPSec védtelen a szolgáltatásbénító (DoS) típusú támadásokkal szemben.

Az IPSec-nek kétféle működési módja van. Tunnel módban (network-network összeköttetés) a teljes eredeti csomag újból becsomagolásra és titkosításra kerül, valamint új fejlécet kap. Ez lehetőséget ad arra, hogy az olyan eszközök, mint például a routerek IPSec proxy-ként funkcionáljanak, azaz a hosztok helyett ezek végezzék el a titkosítást, és a dekódolást. A tunnel módban az IPSec-et alkalmazó gépek átjáróként funkcionálnak és akárhány, logikailag az átjáró mögött elhelyezkedő gép forgalmát képesek továbbítani a tunnelben. A kliens gépeken semmilyen IPSec-hez kapcsolódó feldolgozást nem szükséges végezni, az egyetlen kritérium, hogy az útválasztó táblájukban szerepeljen a megfelelő IPSec átjáró címe. Ez a módszer nagyobb védettséget nyújt a forgalomelemzés ellen, mivel az eredeti fejlécek is rejtve maradnak, így a támadó nem tudja, hogy pontosan hova voltak címezve a csomagok, csak azt, hogy melyik két átjáró között mentek át (még azt sem tudja megkülönböztetni, hogy konkrétan az átjárónak szóltak, vagy a logikailag a mögött elhelyezkedő gépeknek). Azonban az átlapolódó, vagy azonos alhálózatok nem köthetőek össze, ezért a címtartományt úgy kell választani, hogy külön-külön alhálózatba essenek az egyes átjárókhoz tartozó gépek.

Transport módban hoszt-hoszt kapcsolat épül fel, amelynek résztvevői kizárólag azok a gépek, amelyek a kapcsolat végpontjai. Gyakorlatilag a hoszt gépek saját maguk biztonsági átjárói. Ebben a módban, csak az IP payload kerül titkosításra, az eredeti IP fejlécek változatlanul maradnak. Ez lehetővé teszi, hogy speciális feldolgozást végezzünk a végpontok között elhelyezkedő hálózatrészen (például QoS-t (Quality of Services)), de ennek megfelelően ez a mód kevésbé ellenálló a forgalomelemzés jellegű támadásokkal szemben. Ennek a módnak az az előnye, hogy csak néhány byte-ot ad hozzá minden csomaghoz.

Az IPSec infrastruktúra alapját az SA-k (Security Associations) adják. Az SA az a pont, ahol a gyártófüggő implementáció és a heterogén környezet találkozik. Az IPSec-ben két SA szükséges ahhoz, hogy biztonságosan hitelesíthessünk egy kétirányú kapcsolatot.

Mindkét SA a következő összetevőkből épül fel:

- Security Parameter Index (SPI), ami egy 32 bites érték, ami megkülönbözteti az egyes SA-kat egymástól, amelyek ugyanazon két végpont között és ugyanazzal a biztonsági protokollal értelmezettek. Ez az adat teszi lehetővé, hogy több SA-t multiplexelhessünk egyetlen átjárón keresztül;
- Cél állomás IP címe, mely lehet unicast, multicast, de akár broadcast cím is, habár manapság a legtöbb gyakorlati megvalósítás unicast címeket használ. A legtöbb gyártó több SA segítségével írja le a pont-multipont jellegű kapcsolatokat;
- Biztonsági protokoll-azonosító, ahol eldől, hogy az SA melyik protokollt alkalmazza, az AH-t, vagy ESP-t. Amennyiben mindkét protokollt szeretnénk felhasználni, úgy mindkét irányban egy-egy plusz SA-t kell életbe léptetnünk, mivel egy SA csak egy biztonsági protokoll-azonosítóval rendelkezhet.

Az IPSec tehát alapvetően három protokollon alapul:

- ESP - Encapsulation Security Payload (titkosítja és/vagy hitelesíti az adatokat);
- AH - Authentication Header (a csomag hitelesítésére alkalmas szolgáltatás);
- IKE - Internet Key Exchange (a kapcsolódási paraméterek megvitatása, beleértve a kulcsokat is).

Az IPSec két szolgáltatást nyújt: hitelesítést és titkosítást. Ezek külön-külön is alkalmazhatóak, de általában vagy csak hitelesítést végzünk, vagy mindkettőt, mivel a

titkosítás alkalmazása hitelesítés nélkül veszélyes (például „man in the middle” típusú támadásra érzékeny).

Hitelesítés csomag szinten történik. Gyakorlatilag arra szolgál, hogy a kommunikáló felek bizonyosak lehessenek abban, hogy valóban attól származik a csomag, akitől azt elvárják és nem lett módosítva az út folyamán, ez nagymértékben megnehezíti az aktív támadásokat. Csak integritást biztosít, nem próbálja más módon védeni a tartalmat.

Titkosítás valamilyen algoritmus segítségével kódolt üzenetet készít az eredetiből, amelyet optimális esetben csak az információra jogosult tud visszafejteni. Ez főként a passzív támadásoktól hivatott védeni. IPSec esetén ez alatt blokk kódolás értendő. A legtöbb esetben a kulcsok automatikusan generálódnak és kerülnek megvitatásra, valamint bizonyos időközönként cserélődnek az IKE protokoll segítségével.

Az AH az IP fejléc és az egyéb fejlécek közé ékelődik be a csomagban. Minden esetben a csomag fejléc tartalmaz egy következő protokoll mezőt, amely megmondja a rendszernek, hogy milyen fejléc után kell néznie. Az IP fejlécek általában TCP, vagy UDP bejegyzést tartalmaznak ebben a mezőben, míg ha az IPSec protokoll alkalmazása esetén a mező értéke AH. Az AH rámutat, hogy a következő fejléc Authentication Header lesz és ez a fejléc pedig már általában TCP, UDP, vagy encapsulated IP csomagfejlécre mutat.

A titkosítással együtt az IPSec fejléc a teljes csomagot hitelesíti is, azaz biztosítja az integritás megőrzését, kivéve azon a mezők esetén, amelyek az útvonal során normál esetben is módosulnak, mint például a TTL mező értéke.

Az ESP alkalmazható hitelesítésre és titkosításra egyaránt, illetve használható AH-val és anélkül. Az RFC két titkosítási módot ír elő, a DES-t, illetve a null titkosítást, valamint a két hitelesítési módot, a kulcsolt MD5-öt és a kulcsolt SHA-t. A hitelesítési algoritmusok tehát megegyeznek az AH-ban használtakkal. Ezeken az algoritmusokon felül az implementáció elkészítője továbbiakat is támogathat. Titkosításra normál DES-t már nem használunk, mivel bizonyítottan biztonságtalan, tehát 'triple DES'-t, vagy röviden 3DES-t alkalmazunk.

Az IKE protokoll az IPSec kapcsolatokat építi fel, miután az alapvető paraméterek megvitatásra kerültek (alkalmazott algoritmusok, kulcsok, kapcsolat élettartamok). Ez az átjárók között az 500-as UDP porton cserélt csomagokkal valósul meg. Az IKE a következő három protokollt kombinálja:

- ISAKMP (Internet Security Association and Key Management Protocol) (RFC 2408) Kezeli a kapcsolatok megvitatását és definiálja az SA-kat, amely leírja a kapcsolati paramétereket;
- IPSEC DOI (Domain Of Interpretation) for ISAKMP (RFC 2407) Az ISAKMP értelmezésének kiterjesztése domain szintre;
- Oakley key determination (RFC 2412) Az Oakley kulcsokat készít a DH (Diffie-Hellman) kulcscsere protokoll alapján.

Az IKE protokoll két fázisra osztható. Elsőben a hoszt-ok hitelesítik egymást egy RSA kulcs segítségével. A két átjáró megvitatja és felépíti a kétirányú ISAKMP SA-t, melyet a második fázisban használnak fel. Egy átjáró pár között egyetlen SA-val leírható több tunnel is. Ennek a fázisnak az RFC alapján két módja van, 'main' mód, illetve a valamivel gyorsabb, de kevésbé biztonságos 'agressive' mód. A második fázisban az ISAKMP SA-t alkalmazva a két átjáró megvitatja a szükséges IPSec SA-kat. Ezek egyirányúak, azaz minden irányban különböző kulcs van használatban, így mindig párokban kerülnek megvitatásra, hogy

megvalósulhasson a kétirányú kapcsolat. Elképzelhető egynél több pár is két átjáró között. Ebben a fázisban is két biztonsági szint áll rendelkezésre. A biztonságosabb a PFS (Perfect Forward Security), ebben az esetben egy támadó hiába szerzi meg a hosszú távú hitelesítő kulcsot ez nem jelenti azt, hogy azonnal képes lenne a rövidtávú hitelesítést is megtörni. Minden egyes alkalommal, amikor új kulcs kerül alkalmazásba újabb sikeres támadást kell végrehajtania. A gyakorlatban ez azt jelenti, hogy ha valaki ma megtörte a rendszerünket és archiválta a tegnapi forgalmat, azt nem lesz képes elolvasni, feltéve ha időközben történt kulcscsere.

A bemutatott technológia alkalmas arra, hogy az ország területén földrajzilag szétszórt kisebb-nagyobb szervezeti egységeket az inhomogén infokommunikációs környezetben – ahol számos internet- és telefonszolgáltató többféle (optikai vezeték, mobil) technológiát alkalmaz – biztonságosan összekapcsolja, információs igényeit kiszolgálja.

FELHASZNÁLT IRODALOM

- Andrew S.Tanenbaum: Számító-géphálózatok – Panem Könyvkiadó 2004., Budapest (ISBN 963 545 384 1)
- NetAcademia – Tudástár (letöltve 2010. július 22. (http://tudastar.netacademia.net/publikacio/cikk/pdf/0208vpn1.pdf)
- Kersch Péter: Virtuális magánhálózatok – BME Távközlési és Médiainformatikai Tanszék egyetemi jegyzet
- Faczek Szabolcs: Virtuális magánhálózatok – Szakdolgozatok (2001.)
- D. Harkins, D. Carell: The Internet Key Exchange (IKE) – rfc2409
- S. Kent, R. Atkinson: IP Encapsulating Security Payload (ESP) – rfc2406
- S. Kent, R. Atkinson: IP Authentication Header – rfc2402

Tóth András
toth.hir.andras@zmne.hu

A ZÁSZLÓALJ INFORMATIKAI RENDSZEREI ALKALMAZÁSÁNAK SZABÁLYAI, AZ INFORMATIKAI TEVÉKENYSÉGEK VÉDELMI FELADATAI

Absztrakt

A zászlóalj informatikai rendszere az alegység állapotára, helyzetére és feladataira vonatkozó, ezzel összefüggő hírek, értesülések, adatok megszerzése, továbbítása, átalakítása (feldolgozása), tárolása, visszakeresése, valamint rendelkezésre bocsátása érdekében végrehajtott tevékenységek összességét hívatott kiszolgálni. A rendszer zavartalan üzemelése szempontjából az informatikai szakállomány minden felhasználó számára kötelező érvényű rendszabályokat dolgoz ki, amelyek maradéktalan betartása mellett csökkenthető, elkerülhető az eszközök, valamint a hálózat meghibásodása.

The IT system of the battalion is able to serve the purchase, the forwarding, the converting and the storage of the news, the information, and the data of the sub-unit's status, position and functions. The IT staff develops regulations to the smooth functioning of the system, which would be adherence for all users to reduce, to avoid the failure of the equipment and net.

Kulcsszavak: *vírusvédelem, illetéktelen hozzáférés, elektronikus információvédelem, titokvédelem ~ virus protection, unauthorized access, electronic information security, privacy*

A SZAKINFORMATIKAI TEVÉKENYSÉG

A szakinformatikai tevékenység speciális szakmai előképzettséget, felkészültséget igényel, és általában e célra külön rendszeresített személyek, vagy szervezeti elemek végzik (vagy végezhetik). A tevékenység körébe tartoznak: az információrendszer szervezése, a rendszerelemzés, a programozás, az informatikai szakanyag és szoftver beszerzése, a technikai karbantartás, a szervízszolgáltatás, a műszaki fejlesztés, a szakellenőrzés, az adatvédelmi és vírusvédelmi eszközök telepítése.

A zászlóalj szakinformatikai szervezet jogát és kötelességeit a dandár G-6[1] főnökség informatikai tisztje és informatikai beosztottja, valamint a zászlóalj informatikai beosztású katonái együttesen gyakorolják.

AZ ÁLTALÁNOS INFORMATIKAI TEVÉKENYSÉG

Az információfeldolgozás körébe vont adatok összegyűjtését, továbbítását, felhasználását, tárolását, visszakeresését és rendelkezésre bocsátását, valamint az egyéb a szakinformatikai, tevékenységek körébe nem sorolható tevékenységeket általános informatikai tevékenységnek nevezzük. Az általános informatikai tevékenységeket a felhasználók és adatszolgáltatók speciális előképzettség nélkül, a szükséges mértékű betanítás, kiképzés után önállóan végezhetik. Szükség esetén a szakinformatikai állománytól kérhetnek szakmai támogatást.

1 Híradó és Informatikai Részleg

Az informatikai védelem

Az adatok védelmére csak az elöljárói intézkedések által engedélyezett, és a központi nyilvántartásban szereplő védelmi eljárásokat szabad alkalmazni.

Az illetéktelen hozzáférés elleni védelem

Adatvédelmi szempontból minősített és nyílt munkahelyeket különböztetünk meg. A katonai szervezet vezetője jelöli ki a minősített adatok tárolására szánt munkahelyet, amelyet be kell bejelenteni a G-6 főnökségség informatikai tisztjénél. Minősített információt csak a bejelentett számítógépen szabad feldolgozni. Az olyan számítástechnikai berendezések részére, amelynek beépített, vagy háttér adattárolója minősített adatot tartalmaz, a munkavégzés ideje alatt folyamatos felügyeletet, azon túl pedig az ügyviteli szerv helyiségének védelmére meghatározott feltételeket kell biztosítani.

Minősített adatokat tartalmazó, fix merevlemezes, mágneses adathordozót meghibásodása esetén polgári vállalatnak javítás céljából átadni tilos. Ezek javítására, megsemmisítésére a vonatkozó, érvényben lévő előírásoknak megfelelően a kijelölt szakinformatikai szerv (területi szerviz, szakszolgálat) intézkedik. A minősített adatokat tartalmazó eszközök javítását polgári vállalat kizárólag a helyszínen, az illetékes szakszolgálat szakmai felügyelete mellett végezheti.[2]

A kihelyezett terminálok és munkaállomások képernyői a rajtuk megjelenített adatokkal azonos minősítésű iratnak tekintendők. Azok aktuális minősítésének felismerhető jelöléséért, valamint annak megfelelő titokvédelméért annak az osztálynak (alosztálynak) vezetője felel, akinél a berendezés üzemel.

Az alkalmazott hozzáférés elleni védelmi eljárásoknak biztosítani kell az informatikai rendszerbe történő illetéktelen behatolási kísérletek megakadályozását és ezek dokumentálását, a hozzáférés-, program- és adatvédelem megvalósítását. A hozzáférés elleni védelemnek biztosítani kell a felhasználók azonosítását, a hozzáférési igény jogosultságának ellenőrzését, a jogosultságnak megfelelő erőforrások igénybevételét, valamint a felhasználónak nyújtott szolgáltatások feljegyzését, naplózását. A programvédelem biztosítja, hogy a felhasználó csak azokat a programokat, utasításokat hajthassa végre, amelyeket a rendszer működtetéséért (felügyeletéért) felelős személy (supervisor, adatbázis adminisztrátor) a számára engedélyezett, és egyben megakadályozza a nem engedélyezett utasítás (például: programmásolás, módosítás, felülírás, törlés) végrehajtását.

Az Internetre ideiglenesen vagy állandó jelleggel rákapcsolt számítógépeken, a Magyar Honvédséggel kapcsolatos adat tárolása és feldolgozása tilos. Tilos az Internetre az olyan számítógép rákapcsolása, amely lokális hálózat tagjaként üzemel. Az Internet igénybevételére csak fizikailag elkülönített számítógépet lehet használni. Minősített, nyílt illetve belső használatra nyilvános adatok Interneten történő továbbítása szintén tilos.[3]

Rejtjelzéssel történő védelem

Az adatok továbbításánál, a védelem hatékonysága érdekében mindig olyan rejtjelző (kódoló) eszközt és eljárást kell alkalmazni, melynek a biztonsági hatékonysága arányban áll a közlemény fontosságával, minősítésével. A katonai szervezetek informatikai rendszereiben a továbbításra kerülő minősített információk védelméhez csak a rendszeresített, a központilag kiadott, illetve az arra jogosult rejtjelző szervek által kidolgozott rejtjelző eszközöket, programokat és kulcs dokumentációkat szabad használni, az eszközökhöz külön-

2 ÁLT/3 HM és MH Titokvédelmi és Ügyviteli Szabályzata

3 A Magyar Honvédség parancsnokának, vezérkari főnökének 81/1997. (HK 20.) intézkedése az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról

külön meghatározott módon. A dandár informatikai rendszerében alkalmazott rejtjelzéssel történő védelmi eljárások bevezetésére, a védelmi eljárásba vonható személyek kijelölésére a dandár parancsnoka külön intézkedik. Rejtjelző eszköz az Internethez nem csatlakoztatható.[4]

Számítástechnikai titokvédelem (adatvédelem, adatbiztonság)

Az adatvédelem célja, hogy az informatikai rendszer adatait csak az módosíthassa, törölhesse, aki az adatokért felelős. A számítástechnikai titokvédelmi felügyelettel összefüggő feladatok elvégzésére a dandár G-6 főnökség információvédelmi tiszt van kijelölve.

A minősített adat adathordozón történő tárolása és továbbítása, vagy szállítása esetén az adathordozó jellegének megfelelő (fizikai mechanikai, hő, vegyi) védelmet kell biztosítani, a mágneses adathordozót óvni kell a közvetlen elektromágneses behatástól.

Az adatállományok megőrzéséért és rendszeres mentéséért, illetve visszatöltéséért az adatállomány létrehozásáért és karbantartásáért az adatgazda felel. Az adatállományok archiválása mindig dokumentációban előírtak alapján történik, programrendszerek megőrzéséhez hasonlóan.

Minősített adatállományok, valamint pótolhatatlan adatok tárolása két-két lehetőleg független adathordozón, egyik példánya számítógépnél, a másik példánya másodlagos adattárban történik. A másodlagos adattárban elhelyezett adatállományok aktualizálásáról, ellenőrzéséről az adatot szolgáltató köteles gondoskodni.

Biztosítani kell, hogy az informatikai rendszerbe csak az arra illetékes személyek léphessenek be. Lehetőleg hardveres és szoftveres úton is biztosítani kell a belépési jogosultságok ellenőrzését, a jogosulatlan belépés kizárását.

Amennyiben a számítástechnikai eszköz felhasználási területe megváltozik, a rajta található minősített adatokat archiválni és az adattárolót formattálással törölni kell.

A számítógépes vírusok elleni védelem

Előre nem látható rendkívüli események (rendszerkatasztrófa, elemi csapás, tűzeset, stb.) esetére az informatikai rendszerek működésének helyreállítására katasztrófatervet kell készíteni. A terv tartalmazza a helyreállítandó rendszerkomponensek kijelölését, a rendszerszoftverek, alkalmazói programok, adatállományok felsorolását, a tartalék (háttér) számítógép kijelölését, a másodlagos adattár helyét, a helyreállítás menetének ütemtervét és a helyreállításra kijelölt személyeket.

Minden olyan munkahelyen, ahol számítógépes hálózat működik, úgynevezett "vírusvédelmi beléptetési pontot" kell létrehozni. A "vírusvédelmi beléptetési pont" egy önálló berendezés, amelyen a programok telepítése előtt minden új programot és adathordozót ellenőrizni, illetve futtatni kell. Másik berendezésben csak az itt hibátlannak talált program illetve adathordozó használható fel.

Az adatvédelmi és adatbiztonsági rendszabályokban meghatározott időközönként, illetve szükség szerint teljes körű (az ismert vírusokra kiterjedő) vírusellenőrzést kell végezni a rendszeresített védelmi szoftverekkel. Az híradó és informatikai részleg negyedévente végez központilag irányított vírusvédelmi ellenőrzést.

A zászlóaljnál a központilag biztosított vírusvédelmi eszközök telepítését a 43. Nagysándor József Híradó és Vezetéstámogató Ezred, Híradó és Informatikai Központ állománya végzi. A zászlóalj informatikai hálózatában csak a Magyar Honvédség által biztosított szoftverek adathordozók használhatók.

Az alkalmazók szakmai felkészítésekor ki kell térni a vírusok elleni védelem rendszabályainak ismertetésére, valamint a védelmi eszközök használatára.

4 43/1994. (HK 09.) kormányrendelet a rejtjeltevékenységről

A vírusfertőzés észleléskor az alábbi intézkedéseket kell tenni:

a. Fertőzött rendszerek izolálása, elkülönítése (az eszköz kikapcsolása, az ott használt adathordozók elkülönítése, használatból kivonása);
b. Az észlelt jelenség feljegyzése;
c. Az illetékes informatikai szakállomány értesítése;
d. Annak kiderítése, hogy honnan és hogyan jutott be a vírus, ha ez lehetséges;
e. A fertőzés azonosítása és a fertőzés megszüntetése;
f. A vírusfertőzéskor és utána megtett ellenintézkedések regisztrálása.

A tűzvédelem

Azok a helyiségek, melyekben informatikai berendezéseket üzemeltetnek eltérő rendelkezés hiánya esetén a "D" tűzveszélyességi osztályba tartoznak. A zászlóalj Tűzvédelmi Tervébe a létesítményeket e sajátosságok alapján kell besorolni, és a vonatkozó rendszabályokat meghatározni.

Az üzemeltető szervezetek vezetői kötelesek gondoskodni arról, hogy a területükön létesített és üzemeltetett berendezések működtetése az előírások szerint történjen.

Az elektromos berendezéseket a munkaidő végeztével áramtalanítani kell. Az üzemeltetési helyen legfeljebb egynapi üzemeltetéshez szükséges papírból készült adathordozó tárolható, valamint tilos a helyiségben tűzveszélyes folyadékot tárolni. A villamos berendezéseket és a villámhárítót háromévenként tűzvédelmi szempontból felül kell vizsgálni. Minden olyan helyiséget, amelyben központi számítógéprendszer, vagy hálózati szerver üzemel halon oltóval kell felszerelni. A többi helyiségeket (szükség szerint) tűzoltó készülékkel kell ellátni. Az alkalmazókat tűzvédelmi oktatásban kell részesíteni. Ki kell jelölni, és szabadon kell tartani a menekülési útvonalakat, valamint a vészkijáratot.

Egyéb védelem

Az egyéb védelem feladata az előző védelmi kategóriákba nem sorolható veszélyforrások elleni védelmi rendszabályok meghatározása. A munkavédelem, az érintésvédelem, balesetvédelem, a vagyonvédelem, az elektronikai felderítés és zavarvédettség vonatkozó rendszabályainak rögzítése.

Az informatikai eszközök alkalmazásakor lehetőség szerint gondoskodni kell az alkalmazói állomány munkavégzéssel összefüggő ártalmainak csökkentéséről. A megfelelően kialakított és elhelyezett bútorzattal, a megvilágítási viszonyok kedvező kialakításával, sugárzás csökkentő eszközök – monitorszűrő, védőszemüveg – alkalmazásával.

Az informatikai eszközöket tartalmazó helyiségeket megfelelő védelmi eszközökkel – ráccsal, biztonsági zárral, pecséttel – kell ellátni, lehetőség szerint tűz és vagyonvédelmi jelzőberendezéssel kell felszerelni, illetve ezeket a rendszereket üzemben kell tartani.

Fel kell mérni az elektromos zavarforrásokat, el kell hárítani, illetve csökkenteni kell hatásukat. A hibás berendezéseket (zavarforrásokat) meg kell javíttatni, megfelelő árnyékolást kell alkalmazni, illetve át kell telepíteni megfelelőbb helyre. Az elektromágneses sugárzás elleni védelem érdekében a mágneses adathordozókat megfelelően árnyékot tároló helyen (csomagolásban) kell tárolni és szállítani.

FELHASZNÁLT IRODALOM

- 166/1990. (HK 23.) MH HVK Hír. és Aut.Csf. együttes intézkedése az információvédelem anyagi-technikai biztosításának megszervezéséről és a közös feladatok végrehajtásáról
- 104/1992. (HK 23.) MH HVK HIRICSF intézkedése a számítógépes rendszer- és alkalmazói programok anyagnemfelelősi teendőinek szabályozásáról
- 11/1995. HM rendelet a katonai vonatkozású állami- és szolgálati titok köréről
- 43/1994. (HK 09.) kormányrendelet a rejtjeltevékenységről
- A Magyar Honvédség parancsnokának, vezérkari főnökének 81/1997. (HK 20.) intézkedése az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról
- ÁLT/3 HM és MH Titokvédelmi és Ügyviteli Szabályzata
- ÁLT/210 MH Informatikai Szabályzata
- 179/2003 (XI.5.) Kormányrendelet
- 180/2003 (XI.5.) Kormányrendelet
- 1995. évi LXV. Törvény az államtitokról és a szolgálati titokról

Jéri Tamás – Pándi Erik – Jobbágy Szabolcs
jeri.tamas@gmail.com – pandi.erik@zmne.hu – jobbagy.szabolcs@zmne.hu

A HÁLÓZATOK VILÁGA[1]

Absztrakt

Jelen közlemény az IT hálózatok alapkérdéseit tanulmányozza.

This publication studies basic questions related to IT networks.

Kulcsszavak: *hálózatbiztonság, IT hálózat ~ network safety, IT network*

BEVEZETÉS

Napjainkban helyi hálózatok mellett, számos internetbe kapcsolt szervert üzemeltetnek, mely tevékenység elképzelhetetlen kiépített védelmek alkalmazása nélkül. Teljes védelem természetesen nem létezik, így fontos megjegyezni nem elég csak és kizárólag a védelemre helyezni a hangsúlyt, komolyan kell foglalkozni a hálózatok elleni támadás lehetőségeivel, majd a tapasztalatok levonása után beépíteni azokat a védekezés mechanizmusaiba. Komolyabban foglalkozni a támadás és védekezés mechanizmusaival nem lehetséges anélkül, hogy megismernénk a hálózatok fogalmát, a létjogosultságát, melyek a törvényszerűségei, milyen tulajdonságai, sajátosságai vannak. Összességében, a hálózatok világát.

FOGALMI ASPEKTUSOK

A meghatározás szerint a hálózat „olyan speciális rendszer, amely a számítógépek egymás közötti kommunikációját biztosítja”.

Tehát egy speciális rendszer, amiből következik, hogy

- egységes, egész, azaz fizikailag, vagy gondolatilag egyértelműen körülhatárolható;
- minden eleme egy közös cél érdekében működik;
- a benne levő tartalom és forma összhangban van;
- a benne levő rendszer elemek (alrendszerek) funkciója és feladata elsősorban a hálózat rendeltetésszerű működésének biztosítása.

A hálózat alkalmazásának létjogosultsága – egyben rendeltetése - a(z)

- erőforrások megosztása;
- adatok (programok, adatállományok, e-mailek stb.) továbbítása;
- távoli számítógépek elérése;
- költségmegtakarítás.

A számítógép-hálózat kialakításának tehát sok előnyös tulajdonsága van, mely a társadalmat e speciális rendszer sokaságának kialakítására sarkallta. Az elmúlt tizenöt évben gombamód szaporodtak az otthoni, munkahelyi, városi hálózatok és velük együtt fejlődött

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

természetesen a világháló, az Internet is. A hálózatok ilyen szintű kategorizálása egybevethető a kiterjedés szerinti csoportosítással, miszerint lehet

- LAN – helyi;
- MAN – nagyvárosi;
- WAN – világméretű hálózat.

Visszatekintve az emberi kommunikáció fejlődésére, először két pont között oldották meg az információ továbbítását, hol az emberi hang használatával, hol a magasba szálló füstjelekkel, vagy éppen a jól látható fény villogtatásával. A nagyobb távolságok áthidalásához azonban további kommunikációs pontok beiktatására volt szükség, melyek a közbenső adattovábbítás szerepét töltötték be, így biztosítva az információ célba juttatását.

A hálózatok alaprendeltetését leegyszerűsítve, az adatok forráshelyről célhelyre történő továbbításáról van szó, mely a kiterjedéstől függetlenül minden esetben egyaránt követelmény. Ehhez ki kellett alakítani egy szabványos hardver és szoftver rendszert melyek együttese egységesen, minden hálózatban biztosítja az alaprendeltetést.

A hálózatban az adatok az információtechnológiában megszokott módon, digitális jelekként továbbítódnak, melyet az aktív és passzív hálózati elemek biztosítanak.

1. A HÁLÓZAT ELEMEI

Hálózati elem minden olyan hálózatba integrált egység, mely időközönként vagy folyamatosan, részt vállal a digitális jel, forrásból célba történő eljuttatásában.

1.1. Aktív eszközök

Aktív eszköz minden olyan hálózati elem, amely saját energiaforrással rendelkezik, és annak felhasználásával a digitális jel tulajdonságába vagy tartalmába aktívan be tud avatkozni.

A hálózat dedikált pontjai azok az egyedi azonosítóval ellátott aktív hálózati eszközök, melyek önálló fizikai azonosítóval rendelkeznek, ezáltal forrás és cél objektumként is részt vehetnek a kommunikációban:

- switch (kapcsoló);
- router (útválasztó);
- modem (modulátor / demodulátor);
- kliens (munkaállomás);
- szerver (kiszolgáló).

1.2. Passzív eszközök

Passzív eszköz minden olyan hálózati elem, mely saját energiaforrással nem rendelkezik, ezáltal csak és kizárólag a digitális jel továbbításában vállal szerepet, a hálózat kommunikációs közege:

- kábelek;
- csatlakozók;
- aljzatok;
- rendezőszekrények.

2. AZ ESZKÖZÖK KÖZÖTTI KOMMUNIKÁCIÓ

„A kommunikáció az információcsere folyamata, általában egy közös jelrendszer segítségével.”[2] A számítógép-hálózatban csak a dedikált aktív eszközök képesek egymással kommunikálni, mely a sikeres kapcsolatfelvétel után hajtódik végre, és a kapcsolat lezárásával végződik. Az eszközök közötti kommunikáció alapfeltételei:

- egymás azonosítása (felismerése);
- kapcsolatteremtő képesség (kérés, válasz);
- közös nyelv ismerete.

3. ADATKÜLDÉS A HÁLÓZATBAN

A számítógép-hálózatban minden dedikált aktív eszköznek van hálózati csatlakozási pontja (hálózati kártyája), ezáltal fizikai (MAC) címe. A cím minden kártyára egyedi, és csak annak ismeretében lehetséges két pont között kommunikációt megvalósítani.

Az eszközök azonosítását tehát a MAC[3] cím biztosítja, azonban rugalmatlansága és nehezen kezelhetősége miatt az adatok továbbítását a TCP/IP[4] alapú kommunikációs modell végzi.

„… definíciónk szerint egy gép akkor kapcsolódik az Internetre, ha ismeri a TCP/IP protokollt, van IP címe, illetve az Interneten levő bármely másik gépnek képes IP csomagokat küldeni.”[5]

A szerzőnek ez a megállapítása teljes mértékben érvényes az általunk bemutatandó Internet alapú hálózatokra is.

3.1. Protokoll

„Az informatikában a protokoll egy egyezmény, vagy szabvány, amely leírja, hogy a hálózat résztvevői miképp tudnak egymással kommunikálni. Ez többnyire a kapcsolat felvételét, kommunikációt, adat továbbítást jelent.”[6]

3.2. IP cím

Az IP-cím (Internet Protocol-cím) egy egyedi hálózati azonosító, amelyet az Internet Protocol segítségével kommunikáló számítógépek egymás azonosítására használnak.

Az IPv4 szerinti IP-címek 32 bites egész számok, amelyeket hagyományosan négy darab egy bájtos, azaz 0 és 255 közé eső, ponttal elválasztott decimális számmal írunk le a könnyebb olvashatóság kedvéért (pl: 192.168.42.1).

Az IPv6 szabvány jelentősen kiterjesztette a címteret, mert a 32 bit, ami a hetvenes években bőségesen elegendőnek tűnt a jellemzően tudományos és kutatói hálózat számára, az Internet robbanásszerű vállalati és lakossági elterjedése nyomán kevésnek bizonyult. Az IPv6-os címek 128 bitesek, és már nem lenne praktikus decimálisan jelölni őket, ezért

2 http://hu.wikipedia.org/wiki/Kommunikáció
3 A MAC-cím (Media Access Control) egy hexadecimális számsorozat, amellyel még a gyárban látják el a hálózati kártyákat.
4 Transmission Controll Protokoll/Internet Protokoll - Átvitel Vezérlési Protokoll/Internet Protokoll
5 Andrew S. Tanenbaum : Számítógép-hálózatok - Panem Kiadó Kft., 2003
6 http://hu.wikipedia.org/wiki/Protokoll_(informatika)

kompaktabb, hexadecimális számokkal írjuk le, 16 bites csoportosításban. (Pl. 2001:610:240:11:0:0:C100:1319)

3.3. ARP (Address Resolution Protocol – címfeloldási protokoll)

A fentebb leírtak szerint a hálózatba kötött dedikált aktív eszközök – hálózati kártyájuk alapján – saját fizikai címmel rendelkeznek, azonban az adatok továbbítása IP cím szerint történik. E kettősség feloldására vezették be az ARP protokollt, mely átjárhatóságot biztosít a kétféle azonosítás között.

3.4. TCP/IP modell

Hivatkozási modell, mely nevét a két legjelentősebb – TCP és IP – protokolljairól kapta. Lényege, hogy a forrásból célhelyre átviendő adatmennyiség csomagokra bontódik, és egymástól függetlenül saját utat járva érkeznek a célba. A csomagok érkezésétől függetlenül az adatmennyiség eredeti formájába rendeződik és használható fel a célhelyen. A TCP/IP modell egy nem túl szerencsés név, melyet gyakran összekevernek a benne alkalmazott protokollokkal.

3.5. Hálózati portok

A hálózati portok a TCP és UDP – mint az adatcsomagok továbbítását végrehajtó – protokollok velejárói, mindkettejük fejrésze tartalmaz egy forrás és egy cél port mezőt. Az adatok továbbítása IP címmel és forrás porttal rendelkező forráshelyről, IP címmel és célporttal rendelkező célhelyre történik. A portok leginkább a hétköznapi értelemben vett ajtókhoz hasonlítanak. Egy személy egyik házból a másik - különálló - házba úgy jut el, hogy az első ház ajtaján kilép, megteszi a két ház közötti távolságot, majd a másik ház ajtaján belépve célba érkezik. Ajtók, azaz portok hiányában az átjárás nem lenne végrehajtható.

3.6. Szerverek (kiszolgálók)

„A kiszolgáló vagy szerver az informatikában olyan (általában nagyteljesítményű) számítógépet, illetve szoftvert jelent, ami más számítógépek számára a rajta tárolt vagy előállított adatok felhasználását, a kiszolgáló hardver erőforrásainak (például nyomtató, háttértárolók, processzor) kihasználását, illetve más szolgáltatások elérését teszi lehetővé.”[7]

A kiszolgálás szoftveres jelentése (szerverprogram) a tevékenység tényére, a hardveres jelentése a tevékenység végrehajtásának minőségére, gyorsaságára, kapacitására, jelenlétére utal.

A szerverprogram működik kisebb-nagyobb kapacitású számítógépeken, célhardvereken (pld nyomtató szerver) egyaránt, és az alábbi tulajdonságokat hordozza magában:

- folyamatos rendelkezésre állás;
- véges számú ügyfél egyidejű kiszolgálása;
- adatfogadás képessége a hálózatban;
- nyitott TCP / UDP port az IP címen.

7 http://hu.wikipedia.org/wiki/Kiszolgáló

3.7. Kliens - szerver modell

A mai hálózatok döntő többsége ezen az elven alapul, miszerint egyszerűbb ügyfél (kliens) gépek egy nagy(obb) kapacitású kiszolgáló (szerver) gép adataival vagy szolgáltatásaival dolgoznak. A kliens és a szervergépet egy hálózat köti össze, azonban a köztük levő távolság változó, lehet egy épületben, egy városban, akár különálló földrészen, de távolság nélkül egyazon számítógépen is.

A szerverprogram portot nyit a kiszolgálón, ezáltal biztosítja a hálózati kapcsolódás lehetőségét, melyhez a kliens program az ügyfél gépen helyi portot nyit, és az összekapcsolódás végrehajtódik. A szerverprogramok portjai szabványosak (pld. webszerver 80-as és/vagy 443-as), míg a kliens programok (pld. böngésző) portjai véletlenszerűek, előre ismeretlenek, ad-hoc jelleggel jönnek létre.

A szakirodalom[8] a szerveren nyitott portot TSAP-nak (Transport Service Access Point – szállítási szolgálat-elérési pont) hívja.

A kliens-szerver modellre igaz, hogy

- a kiszolgáló és az ügyfélprogramok párban működnek, azonos protokollok szerint;
- a kiszolgáló és az ügyfélprogram közötti kommunikáció normál vagy titkosított;
- a szerver nyitott portjáról – általában – lehet következtetni a kiszolgálás típusára;
- egy szerveren több kiszolgálóprogram is működhet.

4. HÁLÓZATOK ÖSSZEKAPCSOLÁSA

A kisebb hálózatok tömeges elterjedésével, igény mutatkozott azok összekapcsolására, hogy a felismert előnyös tulajdonságok kiterjeszthetők legyenek. Ezt a jogos igényt végül az átjáró (gateway) csomópont hálózatba iktatásával oldották meg, mely úgy képes összekapcsolni két helyi hálózatot, hogy egyszerre mindkettőnek tagja, azaz mindkettő hálózati forgalmában részt tud venni.

A kiterjesztéssel, a klasszikus értelemben vett hálózat jelentése megváltozott, az így összekapcsolt rendszereket internetwork-nek vagy röviden internetnek hívjuk. A kiterjesztés nagyságát figyelembe véve értelmezzük a LAN, MAN, WAN hálózatokat.

5. INTERNET

„Az internet a számítógép hálózatokat összekapcsoló globális rendszer, amely a szabványos internet protokoll (TCP/IP) révén felhasználók milliárdjait kapcsolja össze. Ennek eredménye egyfajta kibertér, amely a valódi világ mellett alternatív teret biztosít. Az Internet a számítógépek összekötéséből jött létre, hogy az egymástól teljesen különböző hálózatok egymással átlátszó módon tudjanak elektronikus leveleket cserélni, állományokat továbbítani.”[9]

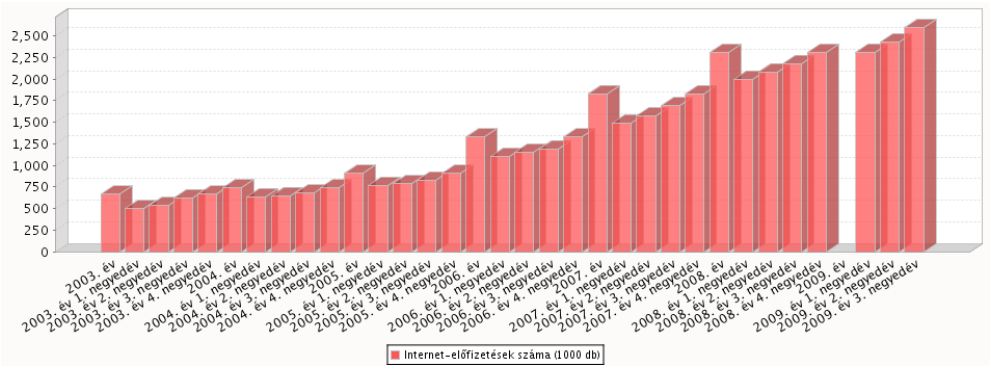
Andrew S. Tanenbaum szerint az Internet nem egyetlen számítógép-hálózat, hanem hálózatok hálózata, a Világháló (World Wide Web) pedig, egy Internetre épülő elosztott rendszer (distributed system). Ezért a számítógép-hálózatok vizsgálatánál nem az Internetet, hanem az Internet felé történő kiterjesztést kell vizsgálni. Véleményünk szerint, ha egy hálózat – bármilyen kis részben is - az Internet segítségével kerül bővítésre, akkor azt a szegmenst kötelező a hálózat részének tekinteni. Az Internetnek kiemelkedő jelentősége van

8 Andrew S. Tanenbaum : Számítógép-hálózatok - Panem Kiadó Kft., 2003
9 http://hu.wikipedia.org/wiki/Internet

a számítógép-hálózatok elleni támadásokban, és - elsősorban - jelenléte teszi szükségessé a védekezést, ezért mindenképpen célszerű részletesebben vizsgálni.

5.1. Az Internet szerepe

Az nem vitatható, hogy napjainkban rengetegen használják, a táblázat szerint 2009. végére több mint 2.5 millió előfizetés volt Magyarországon, és miután gyakoriak az Internet megosztások, a tényleges felhasználók száma ennek többszöröse.



1. ábra: Internet előfizetések változása
Forrás: KSH

A hálózatok támadása – védése szempontjából annak van jelentősége, hogy miként terjesztődnek ki a lokális hálózatok az Internetre, ezért a nagy felhasználó csoportokat külön vizsgáljuk tevékenységük, valamint az Internetre eső hálózati szegmensük szerint:

- háztartások

Valamely szolgáltatótól kapott csatlakozási lehetőséggel kapcsolódnak az Internethez. Több otthoni számítógép, vagy közeli szomszéd esetén helyi hálózat kialakítására kerül sor, és átjáró segítségével kapcsolódnak az Internethez, egyébként egy munkaállomásról direkt csatlakoznak. Tevékenységük során elsősorban az Internet adta szolgáltatásokat használják ki, böngésznek, leveleznek, kommunikálnak, adatokat töltenek le. Esetenként a személyes, vagy családi weblapot is karbantartják, amennyiben az létezik és szükséges az információk frissítése.

- cégek

Vállalati hálózatot hoznak létre, melyet a cég működéséhez (működtetéséhez) használnak. Előfizetés segítségével a hálózatot csatlakoztatják az Internethez, ezáltal a belső hálózatban dolgozóknak biztosítják, hogy munkájuk elvégzéséhez információt szerezzenek, levelet küldjenek és fogadjanak, kommunikáljanak az Internet segítségével, de egyúttal a belső hálózati programokat is használják. Amennyiben a cégnek saját weboldala van, úgy azt is karbantartják, frissítik, adatokat töltenek fel.

- közszféra

Az információtechnológia (IT) mára teljesen beépült a közszféra vérkeringésébe. Mindenhol kiemelt szempont az elektronikus adatkezelés, egyes munkaköröket nem is lehet számítógép nélkül ellátni. Alapkövetelmény valamilyen információs infrastruktúra megléte, melyben az előírt programokkal végzik a napi feladatokat. A költségvetési szerv rendeltetése szerint, gyakran a munkahelyi hálózat is WAN szintű, hiszen országos szervezet esetén (pld. rendőrség, okmány irodák) az ország minden pontján egyaránt szükség van az információra.

Az Internet elérése szinte alapkövetelmény, sok esetben felsőbb szintű jogszabály írja elő az Egységes Kormányzati Gerinc (EKG) használatát, és az információk nyilvánosságra hozatalát (pld egészségügyi intézmények várólistája).

Az Internetet tehát alapvetően - hasonlóan a kliens – szerver modellhez – a szolgáltatások igénybevételére és a szolgáltató tevékenységre használjuk. Megfigyelhető, hogy a háztartásoktól a közszféra felé haladva, csökken a szolgáltatást igénybe vevő és nő a szolgáltatást végző tevékenység, és egyre nő a hálózatok Internetes kiterjedése.

Napjainkban egyre terjed a „homeoffice" típusú munkavégzés, amikor az Internet – mint közeg - kihasználásával a háztartásból jelentkeznek be a céghez, és kvázi a munkahelyi hálózat részeként dolgoznak. Fordított eset is előfordulhat, amikor a lakóhely - IP alapú - vagyonvédelmi rendszerének állapotát, a munkahelyről nézi meg tulajdonosa az Internet segítségével.

5.2. Szolgáltatás igénybevétel vs. végzés

„A szolgáltatás olyan, kézzel nem fogható eredményű munkavégzés vagy jogosultság, mely annak fogadója, vagy élvezője számára értékkel bír, még ha nem is feltétlenül fizet érte."[10]

A hálózati szolgáltatás olyan, az informatikai hálózat valamely dedikált pontján működő tevékenység, mely a hálózat aktív elemei között közvetlenül vagy közvetetten adatcserét tesz lehetővé.

A számítógép-hálózatok támadása és védelme szempontjából az egyik leglényegesebb szempont, hogy a szolgáltató tevékenység valójában hol folyik? A szomorú tény, amit a laikus felhasználók igazán fel sem fognak, hogy direkt, vagy indirekt módon bárhol. A klasszikus szerverprogramok (pld. webszerver) mellett a munkaállomásokon futó programok is gyorsan kiszolgálókká válhatnak.

A mai kommunikációs szoftverek gyakran egyszerre szolgáltatást végző és igénybe vevő tevékenységet is folytatnak, hisz a csevegő, a hangátviteli, a képátviteli stb. programok egyik pillanatban ügyfélként másik pillanatban szolgáltatóként üzemel(het)nek.

Az Internet használat tehát nagyon veszélyes, hisz a belső hálózatban működő munkaállomás kiszolgálóvá válása esetén elérési ponttá változik, melyről a LAN további kiszolgálói is elérhetők.

5.3. Internetes kiszolgálás

A háztartások részére még kismértékben, de a cégek és a közszféra számára kiemelkedő fontosságú az Internetes közönség nagyszámú kiszolgálása. A weboldalak látogatottsága profitot hoz, ezért biztosítani kell a megfelelő szerver-kapacitást és sávszélességet. Előbbi megfelelő hardverválasztással, utóbbi a szerver nagy sávszélességbe helyezésével biztosítható, melyet erre a szolgáltatásra szakosodott vállalkozások kínálnak. A szerverhotelek gigabites Internet hozzáféréssel rendelkeznek, melyek kellő sávszélességet biztosítanak az ott elhelyezett szervereknek, azonban e konstrukciónak hátránya a távoli elérés.

A teljes körű adminisztrálást távolról kell megoldani - valamilyen hálózati szolgáltatáson keresztül -, ugyanakkor figyelni kell a biztonságos üzemeltetésre is. Az adminisztrálás az elszeparáltság miatt általában egy Internet kapcsolattal rendelkező LAN-ból történik, mely idő alatt a szervert és a klienst egy hálózatban levőnek kell tekinteni.

10 http://hu.wikipedia.org/wiki/Szolgáltatások

6. A SZOLGÁLTATÁS CSAPDÁJA

Az angol „service” szó magyarra fordítva egyaránt jelent kiszolgálást és szolgáltatást. Egymással rokon értelmű szavak, van is közöttük átfedés, azonban főleg az informatikában mégiscsak markánsan eltér a jelentésük. A kiszolgálás egy állandó, ingyenes rendelkezésre állás, míg a szolgáltatás olyan rendelkezésre állás, melynek teljesítése - általában - valamilyen feltétel függvénye. A kiszolgálásra jó példa a hálózatba kötött hardver eszköz, mely állandóan, az érkező csomagokat várja, a szolgáltatásra pedig az FTP[11] szerver program, mely csak a jogosultaknak biztosítja az állományok átvitelét a hálózaton keresztül.

A szolgáltatási tevékenységben a kiszolgálóval ellentétben, fellelhető az emberi tényező:

szolgáltató (ember) → számítógép → ? ← számítógép ← igénylő (ember)

A szolgáltató és igénylő ember egymással megegyeznek, elfogadják egymás feltételeit, és megbeszélik, hogy szolgáltató számítógépének kérdésére milyen választ kell adnia igénylő ember számítógépének, hogy a két eszköz együtt tudjon működni. A szolgáltatás igénybevétele tehát - alapértelmezésben - nem jár minden embernek, feltételhez kötött. A helyzetet bonyolítja, hogy a feltételt emberek szabják, a szolgáltatást azonban számítógépek adják és veszik igénybe, tehát a digitális térre kell leképezni az emberi akaratot. Ennek az ellentétnek a feloldására találták ki az autentikációt, mely digitális formára alakítja az azonosítás folyamatát. Szolgáltató (ember) számítógépe akkor szolgája ki igénylő (ember) számítógépét, ha az, az autentikáción megfelel. Ugyanakkor nagyon fontos kiemelni, hogy a számítógépek, csak és kizárólag a rájuk programozott eljárás erejéig képesek hitelesítést végezni, azon túl nem áll módjukban a személyeket azonosítani. Gyenge autentikációs eljárás esetén, könnyen jogosulatlan embernek a számítógépe is igénybe veheti a szolgáltatást, amennyiben megszerzi a szükséges hitelesítő kódokat (pld. jelszavakat, kulcsokat).

A szolgáltató tevékenység - tehát - a kliens-szerver modell elengedhetetlen része, azonban mindig fontos megjegyezni, hogy egyben támadási felület is. A csapdahelyzetet éppen az jelenti, hogy a társadalom elkényelmesedése összetett szolgáltató tevékenységre ösztönöz, ami folyamatosan gyengíti a biztonságot. Példaként a bankok internetes e-bank szolgáltatása egy költségtakarékos, kényelmes pénzkezelési lehetőség, de vajon milyen alapszolgáltatásokból tevődik össze?

- web-szerver az elérhetőség miatt (https://www.xbank.hu);
- smtp-szerver az üzenetek kézbesítéséhez;
- adatbázis-szerver a tranzakciók végrehajtásához;
- sms-szerver a biztonságos hitelesítéshez.

Bármelyik szolgáltatás kiesése az e-bank működését akadályozná, működése viszont támadási pontot jelent.

7. BELSŐ HÁLÓZATOK JELLEGZETESSÉGEI

A LAN-ok összekapcsolásával, illetve az Internet elterjedésével a belső hálózatok kiemelt jelentőséget kaptak. A „belső” szó egyfajta zártságot, elkülönítettséget, homogenitást tükröz, és vele párhuzamosan az informatikai szakmában az adatok védettségére is utal. A belső

11 File Transfer Protocol – Állomány Átviteli Protokoll

hálózatokban rengeteg érzékeny adat fordul elő, melyeket sokan próbálnak támadni, mások pedig – erősen – védenek, ezért célszerű tulajdonságaikat vizsgálni.

- zárt belső hálózatok

Olyan hálózatok, melyek fizikailag semmilyen kapcsolatban nincsenek az Internettel, onnét adatokat se közvetlenül, se közvetetten nem lehet ki,- bejuttatni.

- félig nyitott belső hálózatok

Az Internet felé fizikai kapcsolódási ponttal rendelkező hálózatok, melyből átjáró segítségével – biztonsági / tűzfal szabályok szerint - adatok küldhetők kifelé, vagy adatok fogadhatók befelé.

- belső kezdeményezésű hálózatok

A belső hálózatból nyitott, de az Internet felöl zárt hálózatok, ezért minden Internetes kapcsolat, belső hálózati kezdeményezés eredményeként jön létre.

- külső,- belső kezdeményezésű hálózatok

Olyan belső hálózat, melyhez az Internet felöl, és amelyből az Internet felé egyaránt létesíthető kapcsolat, ezért nagyobb biztonsági kockázatot jelent.

8. HÁLÓZATOK TÖRVÉNYSZERŰSÉGEI

A hálózatok haszna megkérdőjelezhetetlen, ugyanakkor kiépítésük után figyelembe kell venni törvényszerűségeket melyek mind a védekezés, mind a támadás szempontjából fontosak:

- egy működő hálózat jó és rossz célra egyformán rendelkezésre áll;
- kiszolgálók és szolgáltatások nélkül nincs adatforgalom;
- a forgalmazott adat valahol célba ér, tárolódik;
- a kiszolgáló tevékenységét biztosító operációs rendszereket karban kell tartani;
- a távoli szervereken az adminisztráció és a biztonság egyaránt fontos;
- ma már elvárás a szolgáltatási tevékenységek működtetése és kihelyezése az Internetre (magyarorszag.hu ; e-bank; e-commerce);
- egy működő hálózatot nem lehet ki-be kapcsolgatni, mert a szervezet működése függ tőle;
- a szolgáltatások bővítése növeli a hatékonyságot, de csökkenti a biztonságot.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A számítógép-hálózatok kialakításának sok előnyös tulajdonsága van, mely a társadalmat e speciális rendszer sokaságának kialakítására sarkallta, egyúttal alakítva át kommunikációs szokásainkat is. Az elmúlt tizenöt évben gombamód szaporodtak az otthoni, munkahelyi, városi hálózatok és velük együtt fejlődött természetesen a világháló, az Internet is, amelyek az előnyök mellett veszélyforrásokat is hordoznak magukban. A hálózatok világának ismerete nélkül manapság a számítógép-hálózatok elleni támadásokkal szembeni védekezés kérdéseit tárgyalni reménytelennek tűnő feladat. Közleményünk ezen alapokat hivatott közreadni.

FELHASZNÁLT IRODALOM

[1] Andrew S. Tanenbaum : Számítógép-hálózatok, Panem Kiadó Kft., 2003

[2] Dr. Haig Zsolt – Dr. Kovács László: Az információs társadalom információbiztonsága, Elektronikus jegyzet, ZMNE, Budapest 2009.

[3] Kovács Péter: Számítógép-hálózatok; Computerbooks, Budapest, 2004.

[4] Négyesi Imre: Az önkormányzatok informatikai stratégiája és a Magyar Információs Társadalom Stratégia összefüggései (Hadtudományi szemle on-line, II. évfolyam (2009) 2. szám, 85-92. oldal HU ISSN 2060-0437)

[5] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia előadás, 2010.03.05.-06.)

[6] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05.-06.)

Kendernay Zsolt – Pándi Erik – Tóth András
kendernayz@mail.ahiv.hu – pandi.erik@zmne.hu – toth.hir.andras@zmne.hu

A KÉSZENLÉTI SZERVEK INFORMATIKAI RENDSZEREINEK HELYZETE, VÁRHATÓ FEJLESZTÉSI IRÁNYAI[1]

Absztrakt

Jelen közlemény a készenléti szervek informatikai rendszerének fejlesztési kérdéseit tárgyalja.

This publication deals with development questions of IT systems at emergency services.

Kulcsszavak: *IT rendszer, katasztrófavédelem, mentők, rendőrség ~ IT systems, disaster management, ambulances, police*

BEVEZETÉS

A hazai készenléti szervezetek az Országos Rendőrkapitányságból (ORFK), az Országos Katasztrófavédelmi Főigazgatóságból (OKF) és az Országos Mentőszolgálatból (OMSZ) tevődnek össze. Feladatukat a törvényeknek, jogszabályoknak megfelelően hajtják végre. Ahhoz, hogy az EU által támasztott követelményeknek megfeleljenek, növeljék gazdaságosságukat, biztonságosabbá, megbízhatóbbá tegyék segítségnyújtási kötelezettségüket, új mentésirányítási koncepció kidolgozása vált szükségessé. Jelen közlemény az ORFK, OKF, OMSZ szolgálat-, bevetés és mentésirányítási rendszereinek informatikai kérdéskörét dolgozza fel.

1. AZ ÉRINTETT SZERVEZETEK RÖVID BEMUTATÁSA

A résztvevő heterogén profilú szervezetek állami feladatot látnak el. Közöttük hatékony együttműködésre, egységes technikai, irányítási alapok megteremtésére, bővítésére van szükség.

Országos Rendőrkapitányság (ORFK- Rendőrség)

A rendőrség létrejötte az ókorig nyúlik vissza. „Az állami rendőrség 1990-ig a Belügyminisztérium részeként tevékenykedett. Akkor jött létre önálló hatóságként - a belügyminiszter irányítása alatt - az Országos Rendőr-főkapitányság (ORFK). A rendőrség történetében jelentős állomás a rendőrségről szóló 1994. évi XXXIV. törvény megjelenése."[2]

„A rendőrség bűnmegelőzési, bűnüldözési, államigazgatási és rendészeti feladatokat ellátó állami, fegyveres rendvédelmi szerv. Központi országos hatáskörű szerve az Országos Rendőr-főkapitányság (ORFK). Területi szervei az ORFK közvetlen alárendeltségében működő rendőr-főkapitányságok, amelyek valamennyi megyeszékhelyén találhatók. Helyi szervei (városi, kerületi) a rendőr-főkapitányságok önálló feladatkörrel felruházott szerveiként működő rendőrkapitányságok. A rendőr-főkapitányság és a rendőrkapitányság szervezetében rendőrőrs szervezhető. A rendőrség működését a Kormány a belügyminiszter

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült
2 Forrás: http://www.b-m.hu/belugy/tortenet/rendorseg_tortenete_1.htm

útján irányítja. A rendőrség személyi állománya hivatásos állományú rendőrökből, köztisztviselőkből és közalkalmazottakból állhat.[3]

A törvény a Rendőrség feladataként a közbiztonság és a belső rend védelmét határozza meg."

Országos Katasztrófavédelmi Főigazgatóság (OKF)

„A magyar katasztrófavédelem a tűzoltóság és a polgári védelem állami feladatokat ellátó szervezeteiből jött létre." „A hivatásos katasztrófavédelmi szervezet 2000. január 1-jén jött létre. Az állami feladatot ellátó szervezet, fő tevékenységei a felkészülési, a veszélyhelyzet-kezelési, valamint a helyreállítási időszakokban jelennek meg. Szervezeti felépítését tekintve háromszintű a szervezet: központi (országos szint), területi, és helyi szintre tagozódik. Folyamatban van az egységes európai ötszintű közigazgatási térségi rendszerhez való igazodás. Feladatait más állami szervekkel, szolgálatokkal, civil szervezetekkel és a helyi önkormányzatokkal szoros együttműködésben végzi."[4]

Országos Mentőszolgálat (OMSZ)

„A második világháború után nem sokkal, 1948-ban alakult meg Magyarország legnagyobb egészségügyi intézménye, az Országos Mentőszolgálat. Az OMSZ jogelődjei a Vármegyék és Városok Országos Mentőegyesülete, valamint a Budapesti Önkéntes Mentőegyesület. Szervezeti tagozódása a Főigazgatóságból, a Mentőszervezetekből, és a Mentőállomásokból áll. Az OMSZ felügyeleti szerve a Nemzeti Erőforrás Minisztériuma. Az OMSZ vezetőjét pályázat alapján a miniszter nevezi ki. Az OMSZ állami feladatként, teljesítési kötelezettséggel ellátandó alaptevékenységei," között megtalálható a sürgősségi betegellátás keretébe tartozó földi és légi mentés, az országos működésű sürgősségi telefonszámhoz kapcsolt szolgálatvezetői rendszer működtetése, tömeges balesetek, elemi csapások és katasztrófák esetén a kárhely felszámolása. Irányítja és végzi az elsődleges egészségügyi ellátást a társszervezetekkel együttműködve. „A jelenlegi statisztikák szerint ma 213 db mentőállomásán 1238 db mentőjárművel- melyből közel 1000 db a futó mentő gépkocsi - és 7684 dolgozójával látja el mentési és betegszállítási feladatát, az ország egész területén."[5]

2. ORFK- RENDŐRSÉG SZOLGÁLAT-IRÁNYÍTÁSI ÉS SEGÉLYHÍVÓ (112) RENDSZERÉNEK (ESR) HELYZETE, VÁRHATÓ FEJLESZTÉSÉNEK IRÁNYAI

A Rendőrség szervezeti megújításának legjelentősebb lépéseként tartják számon a Határőrség és Rendőrség integrációját. Emellett azonban igen jelentős szereppel bír a működés megújítása, a feladathoz rendelt erő és eszközállomány hatékonyabb alkalmazása is.

A jelenlegi helyzet bemutatása

A Rendőrség különböző pályázatok, projektek révén biztosítja szervezeti és informatikai rendszereinek modernizálását, bővítését, fejlesztését. Több projektben, programban, akár párhuzamosan is részt vesznek, mint például az Egységes Digitális Rádió-távközlő Rendszer (EDR), a Külső Határok Alap vagy az Elektronikus Közigazgatás Operatív Program (EKOP). Az EKOP keretében kapcsolódnak az „Önkormányzati Térfigyelő Rendszerek"

3 Forrás: http://www.freeweb.hu/rendorseg/arendorsegfeladatai.html
4 Forrás: http://www.katasztrofavedelem.hu/tartalom.php?id=1
5 Forrás: http://www.mentok.hu/page.php?newmenuid=9

projekthez is. Ennek a programnak a keretében kívánják megvalósítani a szolgálat-irányítási és segélyhívó rendszer (ESR) korszerűsítését, fejlesztését.

2.1. Szolgálat-irányítási rendszer

A Rendőrség szolgálati ágainál az 1980-as évek óta gyakorlatilag sem a szolgálat irányításában, tervezésében, szervezésében, sem pedig az egyes tevékenységek dokumentálásában nem történt lényegi változás, kivéve a szolgálati munkaidő rendszert, vagyis a szolgálati napló programot.

A helyi ügyeleteket kivéve pontos adat nem áll rendelkezésre a szolgálat aktuális létszámáról. Semmilyen adat nincs az adott pillanatban átcsoportosíthatókról, arról, hogy konkrét időpontban hol, mely területen, milyen eszközökkel, elérhetőséggel állnak rendelkezésre „szabad" rendőri erők. Minden rendőrkapitányság a saját területén irányítja a feladatok végrehajtását, időnként sorolva a bejelentésekre történő reagálást. Lehetséges, hogy a szomszédos területen van szabad járőr, de erről az intézkedő ügyelet nem rendelkezik információval.

A közrendvédelmi, közlekedési ügyeletek adminisztratív terhei is megnövekedtek, és a kézírással vezetett okmányok is nehezítik a visszakeresést, vagyis a korrekt adatszolgáltatás kétséges.

A szolgálat-irányítási központok (ügyeletek) 22 db nyilvántartást vezetnek, és személyes adatokat is kezelnek, melyeknek az előírások szerint, egyértelműnek, hiánytalannak, aktuálisnak kell lennie, valamint törekednie kell arra is, hogy az érintettek adatait csak meghatározott ideig (a tároláshoz szükséges ideig) lehessen azonosítani.

A szolgálatszervezési program, illetve szolgálati napló program, nem egy egységes folyamat része, hanem külön-külön részelemek.

Az egységes EDR rádiórendszer működése lehetővé teszi a járőrök helyzetének pontos meghatározását, ezáltal az esemény helyszínéhez a legközelebbi, az intézkedésre alkalmas járőr vezénylését.

2.1.1. A Rendőrség jelenlegi szolgálat-irányítási folyamatai, szervezeti keretei

A Rendőrségnél jelenleg működő irányítási és információs rendszer felépítése a rendőrőrsök ügyeletétől elindulva, több lépcsőn keresztül jut el az országos rendőr-főkapitányság központi ügyeletéig, majd az előírtaknak megfelelően az Igazságügyi és Rendészeti Minisztérium főügyeletéig.

Az információk, amelyek a rendészeti, bűnügyi szervek által végrehajtandó feladatok megkezdéséhez szükségesek, ugyanezen a rendszeren keresztül jutnak el a vezetői szintekről a végrehajtói állományhoz.

2.1.2. Az ESR (112 –es Segélyhívó rendszer)

Hazánkban több egymás mellett működő segélyhívó rendszer is létezik. Megtalálható az európai segélyhívó vonal (112), mellette párhuzamosan az úgynevezett nemzeti segélyhívó számok (104, 105, 107). Ezeken keresztül teszik meg bejelentéseiket az állampolgárok a Rendőrség, a Tűzoltóság (esetleg a Katasztrófavédelem) és az Országos Mentő Szolgálat felé.

Jelenleg a segélyhívó rendszer stabil, de már előfordulnak olyan gondok, amelyek a túlterhelt informatikai háttérre és az erőforrás hiányára vezethetőek vissza. A 112-es segélyhívások egységes és központi kezelése ezeken a problémákon is segítene.

Szervezeti keretei

A 112-es budapesti segélyhívások a Rendőrség Központi ügyeletére, a jelenlegi Segélyhívó Központba futnak be, a vidéki hívások pedig a megyei rendőr-főkapitányságok ügyeleteire.

2.2. Várható fejlesztések

A rendőrség célja országos elektronizált szolgálat-irányítási képesség megteremtése, - érintve a megfelelő szervezet és folyamat elemeit -, valamint az általa üzemeltetett 112-es szolgáltatás és feldolgozó rendszer korszerűsítése, a társszolgálati készenléti szervezetek rendszerei közötti elektronikus kapcsolat előkészítése, és az állampolgároknak nyújtott szolgáltatások minőségének javítása.

2.3. Jövőbeni elektronizált szervezeti keretek, kapcsolatok

A Rendőrség segélyhívó központja, a szolgálat-irányítási központok, és a rendőrkapitányságok közötti információáramlás elektronikus formában valósul meg. A Rendőrség a fejlesztések során elektronikus kapcsolódási felületek kialakítását is tervezi, melyek a Mentőszolgálat, Tűzoltóság, Katasztrófavédelem és más releváns szolgálatok felé biztosítanának összeköttetést.

A 112-es üzemeltetését továbbra is saját hatáskörében tartaná, de a fejlesztések, szolgáltatások bővítése révén egyrészt lehetősége adódna, azon segélykérések átirányítására, melyek nem a Rendőrség hatáskörébe tartoznak, másrészt továbbíthatóvá válna a segélyhívó központ által lekérdezett esemény-adatlap, harmadszor elérhetővé tennék a társkészenléti szervezetek hasonló informatikai rendszerével való összekapcsolódását, mely – álláspontjuk szerint- a magyarországi segélyhívás-kezelését és az intézkedések hatékonyságát nagymértékben növelné.

A Rendőrségnél tervezett fejlesztéseket során, tehát létrejön a 112-es segélyhívó és szolgálat-irányítási központ, a segélyhívó központok támogató rendszere (ESR) és a szolgálatirányítást támogató rendszer. Elektronizálttá válik a segélyhívó központ, a szolgálat-irányító központ és a Rendőr-kapitányságok ügyeletek közötti kapcsolat, létrejönnek a fővárosi és megyei szolgálatirányítási központok és az irányítási rendszer, valamint előkészítik a készenléti szervezetek hasonló rendszereivel való elektronikus összeköttetést.

Amennyiben ezek a fejlesztések megvalósulnak, nagymértékben nőhet a Rendőrség megítélése, hiszen az állampolgárok számára nyújtott a mentési, segítségnyújtási tevékenység minőségi javulást eredményez.

3. AZ OKF KATASZTRÓFAVÉDELMI OPERATÍV TEVÉKENYSÉGIRÁNYÍTÓ ÉS HATÓSÁGI ELJÁRÁSOK ELEKTRONIKUS ÜGYINTÉZÉSÉT TÁMOGATÓ RENDSZER HELYZETE, VÁRHATÓ FEJLESZTÉSI IRÁNYA

A 2000 évben létrejött szervezet integrálódott a készenléti szervezetekbe és igyekszik megteremteni a működéséhez szükséges feltételeket mind szervezeti, mind technikai szinten. Katasztrófavédelmi faladatának ellátásához folyamatos fejlesztéseket hajt végre.

A jelenlegi helyzet bemutatása

A katasztrófavédelem bonyolult sokténye zős feladat (természeti, biológiai, vegyi, stb.) Mindezen feladatok elvégzéséhez elengedhetetlen egy szervezetileg, technikailag, műszakilag és informatikailag hatékony infrastrukturális háttér.

A katasztrófavédelem szervezeti keretét tekintve 3 szintre bontott. Az első a központi (országos) szint – Országos Katasztrófavédelmi Főigazgatóság, a második a területi szint - Megyei katasztrófavédelmi igazgatóságok, Fővárosi Polgári Védelmi Igazgatóság, Repülőtéri Katasztrófavédelmi Igazgatóság, a harmadik a - Hivatásos önkormányzati tűzoltóságok (HÖT), Önkéntes tűzoltóságok, Polgári védelmi kirendeltségek, irodák.

Az OKF „fiatal" szervezetként folyamatosan teremti meg azokat a műszaki (távközlési és informatikai) feltételrendszereket, ami feladatai ellátásához szükségesek.

Vezetékes híradás területén az OKF korábbi Siemens Hicom 300E központját Hicom4000 HiPath típusúra cserélték. Bevezették a hang/adat integrációs szolgáltatást. A megyei igazgatóságokon Siemens Hicom3500 HiPath típusú központok lettek telepítve.

Folyamatosan történik a veszélyes ipari üzemek környezetében az úgynevezett MoLaRi rendszer kiépítése, valamint a vezeték nélküli URH és EDR rendszerek váltása. 2007-ben csatlakoztak az Egységes Kormányzati Gerinchálózathoz (EKG).

Kialakították a Katasztrófavédelmi Térinformatikai Rendszer (KATIR) meta adattárát. Megkezdték a KÜIR-KATIR rendszerek adatbázisainak integrációját. Frissítették a DSM-2003/10 digitális térkép adatbázisát. Módosítottak a Központi Ügyeleti Információs Rendszer (KÜIR) bizonyos adatszolgáltatási moduljait. Bővítették a LOTUS NOTES vezetői irányító rendszerének (Lotus Notes) felhasználói körét. Véglegesítették az ESR-hez kapcsolódó 22 katasztrófavédelmi tevékenységirányító központ (TIK) helyszínét, infrastrukturális feltételrendszerét.[6] A TIK helyszínek a következők: 19 megyei katasztrófavédelmi igazgatóság (MKI), Fővárosi Tűzoltó parancsnokság (FTP), Fővárosi Polgári Védelmi Igazgatóság (FPVI), Országos Katasztrófavédelmi Főigazgatóság (OKF).

3.1. A katasztrófavédelem infokommunikációs háttere

Az Országos Katasztrófavédelmi Főigazgatóság Informatikai és Távközlési főosztálya végzi mindazon infokommunikációs feladatokat, melyek az OKF informatikai és távközlési tevékenységének biztosításához szükségesek. Üzemelteti és felügyeli Rádiórendszerüket, a Lakossági Riasztó és Tájékoztató Rendszereket, a Balatoni Viharjelző Rendszert (BVR) és a Velencei-tavi Viharjelző Rendszert (VVR), a Dunai Információs Segélyhívó Rendszert (DISR), a Tiszai Információs Segélyhívó Rendszert (TISR), működteti a Katasztrófavédelmi Országos Információs Rendszert (KOIR), a Központi Ügyeleti Információs Rendszert (KÜIR), a Katasztrófavédelmi Térinformatikai Rendszert (KTIR). Ezen kívül előkészíti az OKF rövid- és középtávú távközlési és informatikai koncepcióit.

Katasztrófavédelmi Országos Információs Rendszer (KOIR)

A rendszer lehetőséget nyújt a gyors és operatív döntés előkészítésében, meghozatalában. Az országos lefedettséggel bíró rendszer, a katasztrófavédelemben érdekelt szervezetek informatikai hátterét fogja össze. Feladatai között a gerinchálózat kiépítése és az alkalmazások fejlesztése is megtalálható.

3.2. Az ESR-be integrálható meglévő katasztrófavédelmi rendszerek

Az OKF kulcsfontosságú feladatának tekinti a 112-es Egységes Segélyhívó Rendszerhez való kapcsolódását. A következőkben azoknak a rendszereknek a körvonalai kerülnek bemutatásra, amelyeken keresztül megvalósulhat az ESR-be való integráció.

6 Forrás: http://www.bajavaros.hu/katasztvedelem/KO/k2008011.pdf/1-7.pdf

Központi Ügyeleti Információs Rendszer (KÜIR)

A KÜIR biztosítja az elektronikus kapcsolattartást, csoportmunkát, adatátvitelt, központi Intranet Portál szolgáltatásokat (Dokumentumtár, Hírlevél, Fórum, stb.), az űrlapalapú adatszolgáltatást.

Katasztrófavédelmi Térinformatikai Rendszer (KATIR)

A törvényi előírásoknak megfelelően rendszerben csak állami térképeket és állami alapadatokat használnak. E rendszerek térképi adatbázisaiban az egységes országos vetületi rendszerben és annak koordinátarendszerében meghatározott, vagy az abba átszámított koordinátákat alkalmaznak. A KATIR-ban lévő digitális térképek a közigazgatási egységek határait település szintig jelenítik meg, és házszám szintű adatokat is tartalmaznak.

Az úgynevezett ArcMagyarország adatbázis az ország közigazgatási határait, belterületeit, irányítószámait, körzeteit, országos közúti és vasúthálózatát, főbb vízrajzi elemeit, valamint képállomány formátumban Magyarország domborzatát is magában foglalja.

Ezen felül rendelkezésre áll még a katasztrófavédelmi erők, repterek, árvizes területek, közigazgatási szervezetek adatai is.

A veszélyes üzemek, és veszélyességi fokozatukra jellemző adatok a Hatósági-baleseti Információs Rendszeren belül találhatók meg.

Az esetlegesen még hiányzó adatokat digitalizálással, illetve koordináta meghatározással biztosítják, vagy más országos adatbázisokból együttműködés keretében kapják.

3.3. Várható fejlesztések

Az OKF – ahogyan a többi készenléti szervezet is – fejlesztéseit pályázatok révén valósítja meg, melyben kiemelt fontosságú szerepet tulajdonítanak a készenléti szervezetek egységes tevékenységirányító rendszerének megvalósítására, ennek 112-es Egységes Segélyhívó Rendszerbe való integrálására, és a veszélyhelyzeti kommunikáció rendszerének kialakítására.

Ezeket elsősorban a térinformatikai fejlesztések és a vészhelyzet kezelésében közreműködő szervezetek, szolgálatok, hatóságok közötti adatkommunikáció gördülékenyebbé tételével kívánják megvalósítani. A bevezetés alatt álló EDR mellett olyan információkat, bejelentéseket, segélyhívásokat fogadó, kezelő és feldolgozó rendszer kialakításán dolgoznak, mely magában foglal egy egységes integrált irányítási platform létrehozását is, vagyis a Katasztrófavédelmi Operatív Tevékenységirányító Rendszer (KOTIR) megvalósítását.

A Katasztrófavédelmi Operatív Tevékenységirányító Rendszer (KOTIR)

Ahogy már korábban jeleztük az OKF az elmúlt évek során folyamatos informatikai fejlesztéseket hajtott végre beleértve a térinformatikai fejlesztéseket is. Erre építve a KOTIR megvalósítása során kialakul egy széleskörűen alkalmazható térinformatikai rendszer, amely kiváló lehetőséget biztosít országos szinten a meta adatbázis hozzáféréséhez, mind a védelemigazgatás, mind pedig a katasztrófavédelemben érintett szervek, szervezetek részére.

A katasztrófavédelem szempontjából elengedhetetlen a térinformatikai szolgáltatások bővítése, mely megkönnyíti a katasztrófavédelemben résztvevők közötti kooperációt és kommunikációt. Az elektronikus adatcsere a katasztrófa elhárításban közreműködők közötti tevékenységet segíti, ugyanakkor megfelel lakossági és egyéb, külső (pl.: uniós) elvárásoknak is. Fejlesztésre kerülnek beavatkozó és operatív irányító szervek

számítástechnikai eszközei. Korszerű hálózati aktív elemekkel, biztonságosabb adat, illetve integrált hang- és adatkommunikációs szolgáltatások válnak elérhetővé a veszélyhelyzet-kezelésben érintett szervezetek részére. A fejlesztések során előkészítik az úgynevezett helyi erők a tűzoltóságok, a polgárvédelmi szervezetek 112-es Egységes Segélyhívó Rendszerbe való integrálását, végrehatják a kommunikációs és veszélyhelyzet-kezelési központ és a megyei operatív központok IT eszközeinek modernizálását, a védelmi bizottságok, operatív törzsek és katasztrófavédelmi ügyeletek riasztó-tájékoztató rendszerének, valamint a hivatásos katasztrófavédelmi szervezetek IT rendszereinek korszerűsítését, feladat-orientált bővítését. Terveik szerint megtörténik a hatósági eljárások elektronikus ügyintézését támogató IT eszközök rendszerbeállítása. Ezen kívül létre kívánnak hozni egy térinformatikára épülő katasztrófavédelmi célú lakosság tájékoztatási portált.

Az OKF jelenlegi helyzetének bemutatása jól tükrözi, hogy a szervezet igyekszik élni a mai kornak megfelelő infokommunikációs lehetőségekkel, melyből többféle lehetőséget is kihasznál. Azonban van még néhány eszköz a mobilkommunikációban (mobil és műholdas helymeghatározó), amelyek alkalmazásával a riasztás, tájékoztatás, adatmenedzsment területén a tűzoltást, műszaki mentést, veszélyhelyzet-kezelést végzők gyors, megbízható és kellő mértékű információkkal való ellátását tudnák biztosítani. Ennek kiaknázását az egységes tevékenységirányító rendszerbe történő integrálásukkal együtt képzelik el. Továbbá a megelőzés és hatékony védekezés érdekében a katasztrófakezelésben résztvevők közös informatikai platformjának (pl. térinformatikai rendszerek egységesítése) kialakításában és a lakossági kapcsolódási pontok megteremtésében is tevékenykednek. Az OKF végrehajtja, az elektronikus szolgáltatások nyújtásához szükséges belső fejlesztések, illetve azokat is, amelyek az Egységes Európai Segélyhívó Rendszer (ESR-112) bevezetéséhez szükségesek.

Hatékony biztonságkezelés nehezen elképzelhető integrált tevékenységirányítás nélkül. Amennyiben ezek a fejlesztések kivitelezésre kerülnek, megerősödik az integrált katasztrófavédelmi rendszer.

4. ORSZÁGOS MENTŐSZOLGÁLAT (OMSZ) MENTÉSI-, BEVETÉS IRÁNYÍTÓ RENDSZERÉNEK HELYZETE, VÁRHATÓ FEJLESZTÉSI IRÁNYAI

Az OMSZ az alkalmazott egészségügyi informatika egyik láncszemeként szintén része az utóbbi években végrehajtott egészségügyi reformoknak. Az egészségügyi reform kérdését illetően társadalmunkban igen eltérő vélemények látnak napvilágot. Az, hogy milyen módon és milyen irányú fejlesztések valósuljanak meg, folyamatosan változnak. Mindezek ellenére úgy tűnik, hogy vannak tendenciák, melyekben egyetértés mutatkozik. Ez pedig a technikai, műszaki színvonallal kapcsolatos kérdéskör.

Az OMSZ jelenlegi helyzetének bemutatása

Az Országos Mentőszolgálat feladatai a sürgősségi betegellátás keretébe tartozó földi és légi mentés, a betegszállítás orvosi rendelvényre, a mentőállomás-hálózat, a földi és légi mentő járműpark fenntartása, a sürgősségi telefonszámokhoz kapcsolt mentésirányítási rendszer működtetése. Ezen kívül közreműködik - a társszervezetekkel együttműködve - a tömeges baleseteknél, elemi csapásoknál, katasztrófák esetén a kárhely felszámolásánál, valamint irányítja és végzi az elsődleges egészségügyi ellátást.

A bejelentés folyamata

Az OMSZ naponta hozzávetőlegesen ezer járművének mozgását koordinálja. Az operatív irányítást a Megyei Irányító Csoportok végzik. Ők fogadják a segélykérő hívásokat, és bejelentéstől függően riasztják a megfelelő felszereltségű mentőjárművet.

A főváros Központi Irányító Csoportja a járművek mozgását papíralapú adathordozón és mágnes táblán követi. Budapesten, egy, a kerületekre felosztott táblára a gépkocsikat szimbolizáló, mágneseket helyeznek. A mentőautókkal folyamatos rádiókapcsolatban állnak, s a táblán aszerint mozgatják a mágneseket, hogy egy jármű éppen az állomáshelyén vagy esetnél van, esetleg már a beteggel tart a kórház felé. A telefonon vagy rádión riasztott egységek, a mentéséről kézzel írott beteglapot és menetlevelet készítenek, amit utólag dolgoznak fel számítógéppel.

Az OMSZ 1999 végén vásárolt számítógépeket, szervereket, azonban minden mentőállomásra nem jutott. 2002-ben modernizálták belső hálózatukat, 2003-ban pedig egy komplex fejlesztési program keretében bővítették és korszerűsítették a mentőállomás-hálózatot, valamint fejlesztették a légi mentést.

2007-ban elindult a mentésirányítási rendszer megújítása, mivel 2006-ban elkészültek az új központok, melyek technikailag és a mentés szakmai szempontjából is elfogadható teljesítményre képesek. Az ország 26 pontján lévő hívásfogadó központokban fogadják a hívásokat, és innen történik a mentésirányítása is. A feladatok megszervezéséhez korszerű eszközök állnak rendelkezésre. A megújult a hívásfogadó rendszer lehetőséget teremt a „vaklárma" kiszűrésére, a bejelentők telefonszámának és a beszélgetés egészének rögzítésére, a régió mentőkapacitásának összehangolt mozgatására. Az OMSZ, ahogyan a többi készenléti szervezet is, használja az EDS-t, valamint az Elektronikus Kormányzati Gerinchálót.[7]

A mentés, bevetés folyamata, szervezeti keretei

A megyei mentőszervezetek, illetve a Budapesti Mentőszervezet területükön önállóan intézik a mentést és a beteg szállítást. Az operatív irányítást a megyeszékhelyi mentőállomás megyei szolgálatvezetője (diszpécser) irányítja, korlátlan intézkedési jogkörrel. Ezen kívül koordinálja a megyén kívülre irányuló betegszállításokat. Tömeges baleset, illetve katasztrófa bekövetkezése esetén azonnal jelentési kötelezettsége van a budapesti Központi Irányító Csoport szolgálatvezető főorvosának.

Budapesten a Központi Irányító Csoporton belül a mentést a mentésvezető mentőtiszt, a betegszállítást a szállítás irányító koordinálja a szolgálatvezető főorvos irányítása mellett, aki egyben az országos operatív irányítás legmagasabb vezetője. A mentést különböző szintű mentőegységeken keresztül biztosítja. A mentés végrehajtásának operatív egységei a mentőállomások, melynek irányítását a szolgálatvezető végzi.

Az egész megye szolgálatirányításáért a megyei szolgálatvezető felelős, aki egyben a mentőszervezet vezető főorvos operatív helyettese is. Ő felelős a mentőállomások, illetve a szomszédos mentőszervezetek között folyó mentési és betegszállítási feladatok összehangolásáért.

A mentőállomásokon a segélyhívás fogadása és a bevetés irányítás egy helyen van. A 104-es vezetékes telefonról a hívás mindig az illetékes mentőállomáshoz fut be, mobiltelefonról a tartózkodás helye szerinti megyeszékhelyi mentőállomásra. Megyeszékhelyi mentőállomáson a szolgálatvezető munkáját telefonügyeletesek is segítik.

4.1. Várható fejlesztések

Ahogy minden más szervezetnek, az OMSZ-nek is szüksége van folyamatos megújulásra, modernizálásra, mind módszertani, mind technikai, műszaki szinten. Mindezeket különböző pályázatok segítségével valósítja meg, melyre igen nagy szüksége van, hiszen a készenléti szervezetek közül – információim szerint – a legelavultabb paraméterekkel rendelkezik. Ez

7Forrás:
http://www.bm.hu/web/belsajt.nsf/0/8E86C2198982943AC12571F00036B0B4/$FILE/OnKo_06_12_online.pdf?OpenElement

lassan változni látszik, hiszen mostanság számára is lehetővé vált, - EU-s pályázat révén- hogy végre kialakíthassa új mentési-, bevetés irányítási rendszerét.

Az OMSZ várható fejlesztési iránya

A hatékonyabb betegellátás irányába ható változtatási folyamat részeként az OMSZ úgynevezett térinformatikai rendszert bevezetését tervezi, ami nemcsak a mentőautók helyzetének meghatározását, vagyis a mentésszervezést segíti, hanem ami talán még fontosabb, a kétirányú digitális adatcsere is lehetővé válik a mentőautók, illetve és központok között. Az új számítógépes bevetés irányítási rendszer automatikus erőforrás-tervezéssel és elektronikus adattovábbítással váltaná ki az eddigi manuális irányítást, vagyis biztosítja a központ és a mentőautók közötti elektronikus kommunikációt, valamint EDR és a GPS (Globális Helymeghatározó Rendszer) használatával folyamatosan nyomon követhetnék a járművek mozgását is.

Az OMSZ tervezett mentésirányító rendszere

A mentés-, bevetés irányítási rendszer hozzájárul a sürgősségi betegellátás alapvető követelményrendszeréhez, mely helytől és időtől függetlenül biztosítja az állampolgári esélyegyenlőséget. Az európai normák szerint, a sürgősségi esetekben a földi mentőknek is a riasztást követő 15 percen belül kell megérkezniük a helyszínre. Az OMSZ ennek az elvárásnak 78 százalékban tud megfelelni. A rendszer megvalósulásával ez az arány jelentősen változhat. Légi mentésnél a jelenlegi 7 légi bázissal (Budaörs, Pécs, Miskolc, Debrecen, Balatonfüred, Sármellék, Szentes) és a nyolc géppel szükség esetén a lakosság nagy része már 15 percen belül helikopteres mentésben részesülhet.

Az OMSZ feladatait megfelelő informatika rendszerrel kívánja lefedni, mely által egy egységes digitális rádiórendszer alapú gépjármű felügyeleti rendszer alakul ki. A digitális adatátviteli rendszer képes lesz on-line adatcserére a mentőkocsi és az irányító központ között. Az irányító központok, a munkahelyek, a mentőállomások és a mobilegységek között működő informatikai háttérrendszer jelenleg nem áll rendelkezésre, ez azonban az új rendszerek közötti kommunikációval pótlásra kerül.

Az OMSZ tervezett mentésirányító rendszerének rövid bemutatása

A OMSZ szerint a jövőbeni rendszer képes lesz minden olyan funkció támogatására, amely növeli a mentéssel, a betegellátással összefüggő feladatok színvonalas teljesítését. Az elektronizálás eredményeként a rendszerben valósidejű adatok kerülnek a hívásfelvételtől az eset lezárásáig.

Az intelligens gépjármű fedélzeti egységek (pl. tablet PC) alkalmazásával a rendszerben megvalósul, az úgynevezett. „elektronikus feladattovábbítás” funkció, valamint lehetőség nyílik az elemzések és kiértékelések, elszámolások azonnali elvégzésére. A rendszer workflow-kezelést biztosít a bevetés speciális tulajdonságainak megfelelően. A rendszerben a szöveges képernyőket térképi megjelenítés egészíti ki.

A vonuló mentő gépjárművek tevékenységét az EDR (Egységes Digitális Rádiórendszer) rendszerbe integrált, GPS alapú gépjármű-felügyeleti rendszer kezeli. A rendszerhez illeszthető a CallCenter típusú telefonközpont már 27 helyen működik. A távoli (webes) lekérdezéssel a rendszer információkat szolgáltat a felső vezetés (megyei és országos szakmai vezetés, EüM) számára.

A rendszer a munkafolyamat minden szakaszában, a bejelentés felvételétől kezdve, a probléma-elhárítást végző csapat személyi és műszaki összeállításán, a segítségnyújtásra, vagy bevetésre indult egység folyamatos térképi követésén, és a helyszíni tevékenységek irányításának támogatásán át, egészen az utólagos elemzésekig, az események pontos

naplózásával, a változó körülményekhez alkalmazkodó dinamikus folyamatkezeléssel, és a speciális, adatbázisban tárolt információk folyamatos rendelkezésre bocsátásával, valamint dinamikus gépjármű-felügyelettel hatékonyan segíti a diszpécser munkáját.

A rendszer multifunkciós, azaz képes párhuzamosan több, eltérő tevékenységet folytató központ kiszolgálására is. Az egyes központok adatait ugyanazon a szerveren, de elkülönítve kezeli. A jogosultsági rendszer biztosítja, hogy minden diszpécser csak a saját részlegének adatait láthassa, a többiekét pedig ne.

A rendszer lehetővé teszi a bejelentés-kezelő, a bevetés moduljai tudásbázisainak és a teljes folyamatot irányító workflow-nak a központonkénti (szervezetenkénti) eltérő feltöltését, mely mindenhol biztosítja a folyamatok testre szabását.

A kliens-szerver felépítésű mentési-, bevetés irányítási rendszer a vastag kliens architektúrának felel meg. Ez alól csak a vezetői munkahelyek kivételek. Itt vékonyabb kliens használatára van szükség, mivel a kliens program nincs telepítve, csak a térképek.

A rendszer felhasználómoduljai a következők:

- Erőforrás nyilvántartó modul;
- Szolgálatvezénylő modul;
- Bejelentés-kezelő modul;
- Bevetési modul;
- Térinformatikai modul;
- Járműkövető modul;
- Berendezés-vezérlő modul;
- Riport modul;
- Webes lekérdező modul.

A fejlesztések összefoglalása

Végül elmondható, hogy az OMSZ az ország 26 pontján korszerű hívásfogadó központokban végzi a mentésirányítást és a beteghez a legközelebbi állomásról, helyismerettel rendelkező mentőautót küldenek. Az OMSZ is csatlakozott az úgynevezett EDR rendszerhez, amely a mentőkocsik mozgásának követésére is alkalmas, valamint biztosítja a központ és a mentőkocsi közötti elektronikus kommunikációt.

Ezen kívül mentési-, bevetés irányítási rendszerfejlesztést hajtanak végre, amely a digitális adattovábbítás és a számítástechnikai eszközök segítségével végzett riasztás feltételeit is megteremti. A rendszer alkalmazásával optimalizálható a mentő erőforrások felhasználása, javítható a segélyhívások, fogadások színvonala (a társszervekkel történő együttműködés képessége), ugyanakkor bevetések alkalmával, csökkenthetővé válik a kiérkezések ideje. Javulhat az események helyszíni tevékenységének, a diszpécsernek szakmai támogatása, tervezhetőbbé válhat a szolgálatszervezési és logisztikai tevékenység. Az OMSZ hívásfogadó és mentésirányító rendszere várhatóan az idén megvalósul.

Meg kell jegyeznünk, hogy az OMSZ-nél kevés utalást találtunk a 112-es vagy az ESR-re utaló elképzelésekre. Az új rendszernél ugyan jelezték, hogy általa optimalizálódik a társszervekkel való kommunikáció, de ezen túlmenően, sem az ORFK-val sem az OKF-el nem látni a témára vonatkozó különösebb együttműködési szándékot. Új információim szerint, azonban úgy tűnik, hogy a közeljövőben ez változik, mivel felsővezetői és szakember szinten is megindul az együttműködés. Az OMSZ felvette a kapcsolatot a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalával is (KEK KH), mely az ERS működtetésével, koordinálásával megbízott intézmény.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Közleményünkben áttekintettük a készenléti szervek ágazati informatikai rendszereinek sajátos fejlesztési irányait. Nyilvánvaló tény, hogy az egységes segélyhívó rendszer tényleges kialakítása és működtetése hazánk számára napjainkra már nyomasztó mulasztássá nőtte ki magát. Rávilágítottunk azon tényre, amely szerint a kínálkozó informatikai, információ feldolgozó, illetve infokommunikációs rendszerek lehetőséget biztosítanak a korszerű tevékenységirányítás megvalósítására.

FELHASZNÁLT IRODALOM

[1] Önkormányzati tájékoztató: Az országos mentőszolgálat tájékoztatója, http://www.bm.hu/web/belsajt.nsf/0/8E86C2198982943AC12571F00036B0B4/$FILE/OnKo_06_12_online.pdf?OpenElement (2010-03-15)

[2] 26/2008. (OT 16.) ORFK utasítás a Rendőrség katasztrófavédelmi tevékenységének egyes kérdéseiről, http://www.police.hu/data/cms536291/26_2008_orfk_ut.pdf (2010-03-15)

[3] MEH - Az egységes európai hívószámra (112) alapozott, Európai Segélyhívó Rendszer (ESR) magyarországi kialakításáról Közzététel: 2007. 02. 01. http://jogalkotas.hu/drupal/node/720 (2010-03-15)

[4] Dr. Tatár Attila: A 112 Egységes Segélyhívó, Rendszer és a tűzoltóságok Országos Katasztrófavédelmi Főigazgatóság kapcsolatának kérdései, http://pro-m.hu/resource.aspx?ResourceID=Dr_Tatar_Attila (2010-03-20)

[5] Dr. Bukovics István – Kiss Ernő – Dr. Papp Antal: Klímafelkészülés és katasztrófavédelem (2004. augusztus) http://www.pkkm.org/klima.pdf (2010-03-29)

[6] Geiger János: A megyei védelmi igazgatás helye és szerepe a katasztrófák elleni védekezés rendszerében, http://www.vedelem.hu/files/UserFiles/File/konf2007/pv/Szatmari.ppt (2010-03-29)

[7] OKF Jogszabályi háttér, http://lakossag.katasztrofavedelem.hu/index.php?pageid=103&content=1 (2010-03-29)

[8] Polgári védelem tájékoztatója, http://pv.battanet.hu/pv1.htm (2010-04-01)

[9] ORFK: szervezeti felépítés, http://www.police.hu/data/cms647663/szervezeti_felepites.pdf (2010-04-05)

Jobbágy Szabolcs – Sándor Miklós
jobbagy.szabolcs@zmne.hu – sandor.miklos@zmne.hu

A MINŐSÍTETT ADATOK VÉDELMÉNEK JOGI SZABÁLYOZÁSA

Absztrakt

Mindenki számára köztudott, hogy a saját maga határait feszegető, a lehetetlent nem ismerő, megállíthatatlanul dübörgő információs társadalom mindennapjainak a szerves, tudatos és aktív részesei vagyunk. Az ezt átívelő információs szupersztráda alappilléreit megtestesítő információ nélkül elképzelhetetlen ennek a pillanatról-pillanatra megújuló infokommunikációs forradalomnak a léte. Lényegi mivolta abban gyökerezik, hogy az információ mindenki számára a megfelelő módon, a megfelelő mennyiségben és minőségben, a szükséges mértékben, a kellő időben és helyen a rendelkezésére álljon. Ebben a milieu-ben az információt a felfokozott jellegéből adódóan azonban nem szabad magára hagyni, védeni kell a rosszakaratú támadások, az illetéktelen és jogosulatlan hozzáférésekkel szemben.
A szerzők a cikkben alapul véve és elemezve a „Minősített adatok védelméről szóló 2009. évi CLV. törvényt" röviden általános kitekintést próbálnak nyújtani az információbiztonságnak, az információvédelemnek, mint egyre markánsabban megjelenő és érvényesülni kívánó, a híradást és informatikát vagy komplex értelemben az új keletű megnevezéssel illetett infokommunikációt és ennek a technológiai alapját megtestesítő infokommunikációs rendszereket-hálózatokat egyaránt akarva-akaratlan és nélkülözhetetlenül átható szakterületnek a hazai szabályozására.

It is common knowledge that we all are integral, conscious and active participants in the everyday life of unstoppably booming information society, which keeps trying to go beyond its limits and for which nothing is impossible. Information, embodying the base of the information superhighway spanning over it, is indispensable for the existence of this infocommunication revolution, renewing itself every single moment. Its essence is that information should be made available for everyone in the proper way, in the proper amount and quality, to the desired extent and at the proper place and time. In this environment, due to its intense nature, information must not be left alone but should be protected against any ill-meant attacks or unauthorised and illegal access.
Taking 'Act No. CLV of 2009 on the protection of qualified data' as their starting-point and analysing it in their article, the authors strive to give a brief and general overview of the national regulation of information security or protection as a more and more markedly present and prevalent field, unavoidably and indispensably penetrating both telecommunications and IT, or in a complex sense and with their newly-coined common name, infocommunication, as well as the infocommunication systems and networks providing the technological base of the former.

Kulcsszavak: *információs társadalom, infokommunikáció, információ, információbiztonság, minősített adat, bizalmasság, sértetlenség, rendelkezésre állás, elektronikus információbiztonság ~ information society, infocommunication, information, information security, classified data, confidentiality, integrity, availability, electronic information security*

ELŐSZÓ

Napjainkban a társadalmi fejlődés fokozatainak harmadik nagy szignifikáns korszakát, ciklusát éljük, melyet az információs társadalom[1] kifejezéssel illet a releváns szakirodalom. Ennek a típusú társadalmi szerveződésnek az alapvető alkotóeleme, legfontosabb lényegi meghatározója az információ[2], mely egy óriási jelentőséggel bíró „érték", mellyel rendelkezni, melynek birtokosának lenni, pedig „hatalom". [1][2][3][4]

Ezen egyszerű okból kifolyólag azonban nem csak az információ értékének, jelentőségének a súlya, hanem a vele szemben megnyilvánuló támadások száma is ugrásszerűen megnőtt és folyamatosan növekvő tendenciát mutat napjainkban is, mely támadások, illetéktelen információszerzések-hozzáférések, a jogosulatlan behatolások változatos formáinak, minden lehetőséget kiaknázó módjainak tárháza határokat nem ismer. Ugyanakkor a fent említett tevékenységek negatív, destruktív hatásai, az általuk okozott károk volumene is egyre súlyosabb következményekkel jár az egyes személyek, az ország, az információt kezelő rendszerek, ezáltal a katonai infokommunikációs rendszerek biztonságának vonatkozásában is.

Ez egyértelműen megköveteli az információ fokozottabb védelmét, a továbbítására, feldolgozására, tárolására, kezelésére szolgáló infokommunikációs hálózatok[3] [5] biztonsági szintjének fokozását, az információ és az átvitelére szolgáló rendszerek védelmére, a biztonságos továbbításnak a lehetővé tételére predesztinált egyre kifinomultabb, megbízhatóbb és biztonságosabb módszerek, eljárások, technológiák, eszközök és berendezések életre hívását és rendszerbeállítását, a szükséges információk-adatok különböző szintű minősítését, az információbiztonság[4] [6], az információvédelem[5], a minősített adatok[6] [7] kezelésével kapcsolatos eljárások, szabályzó intézkedések, törvények,

1 Információs társadalom: Egy viszonylag új keletű dolog, mely az informatika és a távközlés konvergenciáján, az információ és a tudás szabad létrehozásán, forgalmazásán, hozzáférésén és felhasználásán alapuló társadalmi struktúra kialakításán nyugszik. Legfőbb mozgatórugója az informatikai, a távközlés, a szórakoztató elektronika, és a média külön – külön is hatalmas ütemű fejlődése. A Hadtudományi Lexikon értelmezésében az ipari társadalmak utáni társadalmi formáció, a XXI. századi úgynevezett információs korszak társadalma.

2 Információ: Átvitelre, tárolásra vagy feldolgozásra alkalmas formában kifejezhető hír, ismeretanyag. Az információ lehet jel, adat, szimbólum, kép, hang, stb.

3 Infokommunikációs hálózat: Az infokommunikáció az informatika és a kommunikáció (híradás) integrációja. Az infokommunikációs (híradó-informatikai) rendszer magába foglalja az információ előállítását, gyűjtését, felvételét, tárolását, feldolgozását, törlését, és továbbítását, továbbá az ehhez szükséges berendezéseket, elektronikus eszközöket, üzemeltető és felhasználó személyeket az információ bármely típusát tekintve.

4 Információbiztonság: „Az információbiztonság a katonai szervezetek vezetésének, működésének sikere érdekében az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az adatkezelő képességek megfelelő szintű védettsége."

5 Információvédelem: Az információvédelem fogalmára nagyon egyszerű magyarázattal szolgálhatunk a hozzá szorosan kapcsolódó fogalom, az információbiztonság alappillélére építkezve. E gondolatmenetet végigfuttatva azzal a triviális megfogalmazással élhetünk miszerint, ha az információbiztonságot egy állapotnak tételezzük fel, akkor az információvédelem ennek az állapotnak a megteremtésére, fenntartására és fokozására irányuló tevékenységek és eszközök összessége.

6 Minősített adat: A 2009. évi CLV. a minősített adatok védelméről szóló törvény értelmében megkülönböztethetünk nemzeti és külföldi minősített adatot. A nemzeti minősített adat „…olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti…és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza." A külföldi minősített adat fogalma, pedig „Az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza."

jogszabályok komplex egységének és az információbiztonság-politikának[7] [6] az előtérbe kerülését.

Az egyre fokozottabb veszélynek kitett infokommunikációs rendszerek-hálózatok, a rajtuk keresztül továbbított információk, minősített adatok azonban nem csak a „polgári-civil" szférában vannak jelen az egyre inkább növekvő „információéhség" és az újabbnál-újabb felhasználói igények kiszolgálásának érdekében, hanem a fegyveres erők, a haderők szektorában, mint egyfajta speciális felhasználási szegmensek területén is aktívan képviseltetik magukat a vezetés és irányítási rendszerek, a csapatok vezetésének legfontosabb és alapvető eszközeiként. Ezen elméleti megfontolás alapján érthető, hogy a katonai kommunikációs rendszerek információbiztonságának kérdése is halaszthatatlan és folyamatos megújulást igénylő és egyben megkövetelő kérdéskör. Különösen igaz ez a mai kor modern hadseregeire, hadviselési módjaira, digitális hadszíntereire[8] [8][9][10]. Ebben a speciális, új típusú környezetben az információ, a különféle katonai infokommunikációs hálózatok óriási jelentőséggel bírnak. A digitális hadviselés[9], a hatásalapú műveletek[10] [10], a hálózatközpontú hadviselés[11] [11], mint az „új típusú küzdelem" alapvető alkotóelemeit testesítik meg az ellenség legyőzése, az információs fölény-uralom megszerzése-kivívása, a kitűzött cél, a meghatározott feladat elérése és véghezvitele céljából többek között digitális katonák[12] [12] és információs harcosok[13][10] bevetése, alkalmazása révén.

7 Információbiztonsági politika: Az információbiztonsághoz szorosan kapcsolódó fogalom. Tulajdonképpen „Az általa meghatározott felelősségi rend és hierarchizált szabályozás, a saját erőkre, képességekre, környezetre, ellenséges erőkre vonatkozó adatok biztonsági alapelvek szerinti kockázatokkal arányos védelme, valamint a rendszabályok folyamatos pontosítása, hatékonyságuk ellenőrzése, a biztonsági eseményekre való gyors és hatékony reagálás képezi az információbiztonság alapját."

8 Digitális hadszíntér: Egy többdimenziós, digitalizált hadszíntér, ahol magas fokon elektronizált, tudás alapú (knowledge based army), nagy találati pontosságú precíziós (hightech) fegyverzetű hadseregek, digitális katonák, információs harcosok harcolnak. Alapvetően infokommunikációs, multimédiás szolgáltatásokat biztosító harci hálózatokon nyugszik, helyet biztosít a támadó és védelmi információs műveleteknek. „Digitális hadszíntér alatt azt a virtuális teret ért(het)jük, amely magába foglalja a fegyveres küzdelem rendszerének informális elemeit (az elektronikus információszerzés, -továbbítás, -feldolgozás illetve az ennek bénítására és lefogására alkalmazott eszközöket és eljárásokat)."

9 Digitális hadviselés: Napjainkban a harmadik hullámú vagy negyedik generációs hadviselés korszakát éljük, mely a 21. század jellemző hadviselési módja. Legfontosabb jellemzője a globalitás, a dinamikus hadműveletek, a vezetés-irányítási rendszerek (C2-Command and Control) pusztítása, precíziós csapások, digitális és hálózatos hadseregek. Alkalmazására elsőként az I. Öböl háborúban került sor a nemzeti kommunikációs és államigazgatási infrastruktúra ellen intézett digitális, infokommunikációs támadások végrehajtása által.

10 Hatáslapú műveletek (effects-based operations): „A katonai műveletekben alkalmazott hatásalapú megközelítés (effects-based approach) elve szerint a hadszíntéren egymással hálózatba kapcsolt objektumok vannak. Egy kiválasztott központ és a benne található nagyfontosságú célpontok elleni támadás, különböző hatásokat eredményezhet a többi, hozzájuk kapcsolt objektumok működésében is….A hatásalapú műveletekben a korábbi felfogáshoz képest komolyan figyelembe veszik azt a láncreakcióhoz hasonlító elvet, miszerint a kezdeti közvetlen hatással –első csapással- törvényszerűen további közvetett károsító, korlátozó hatásokat lehet elérni, amely a teljes rendszerre különböző mértékű negatív hatást fejt ki. Az előidézett hatások eredőjének, vagyis az összhatás eredményének elemzése és értékelése képezi a hatásalapú műveletek lényegét….A közvetlen és közvetett hatások elve szerint egy rendszer belső – kulcsszerepet játszó – elemeire mért pusztító vagy korlátozó jellegű csapás mind a rendszeren belül, mind, pedig a rendszerek közötti kapcsolatokban másod, harmad és n-edik típusú és erősségű hatásokat vált ki."

11 Hálózatközpontú hadviselés: „A hálózatközpontú hadviselés (NEC- Network Centric Warfare) legfontosabb eleme az információk megszerzésének és felhasználásának radikálisan új módja, amely gyökeresen átalakítja a haderő vezetési rendszerét is, hiszen lehetővé teszi, hogy minden információ a vezetés minden szintjén egy időben álljon rendelkezésre, és ennek megfelelően a döntések mindig a lehető leggyorsabban és a döntés szempontjából optimális szinten szülessenek. A NEC lényege, hogy egyetlen integrált rendszerbe foglalja az érzékelőket, a döntéshozókat és a fegyverrendszereket. Alkalmazása során kiemelkedő jelentőségű a koalíciós partnerek közötti minél jobb információ-megosztás, a döntéshozatal felgyorsítása, illetve az, hogy a megfelelő időben a megfelelő katonai eszköz kerüljön bevetésre. Az NEC sokkal több, mint többletfelszerelés: optimalizált parancsnokságra, vezetési struktúrára, illetve átalakított kiképzési rendszerre helyezi a hangsúlyt, hogy a válasz gyors és a körülményeknek megfelelő legyen."

12 Digitális katona: „A digitális katonák (vagyis összfegyvernemi manőverező erők) a digitalizált harcmezőn, elektronizált és informatizált fegyverrel, digitális vezérlésű, igen nagy találati pontosságú ún. precíziós fegyverrel harcolnak az általános hadműveleti terv alapján. Kiképzésükbe és felkészítésükbe beletartozik a számukra

Mielőtt hozzálátnánk a címben megnevezett törvény boncolgatásához, fontosnak tartom összegezvén a fent elhangzottakat tisztázni azt a kérdést, hogy hogyan is kapcsolódik össze az információ, az infokommunikációs hálózat az információbiztonság és a minősített adatok védelmének a kérdésével. A közös csatlakozási pont evidens, hiszen mint azt korábban említettük volt egy fogalmi kitekintő keretében, az információ számtalon formában van jelen az őt továbbítani, feldolgozni, tárolni predesztinált infokommunikációs rendszerben, mint például hang, kép, jelzés és a számunkra, a cikk szempontjából meghatározó jelentőséggel bíró adat formájában. Tehát az adat tekinthető úgy is, mint egy ismeretelem, egy valamilyen információt magában hordozó, az információ, mint értelemmel bíró adat, „infokommunikációs elem", melyet tartalmának függvényében minősíteni, az adathoz való hozzáférést a szükséges és elégséges mértékben korlátozni kell, az adatot védeni kell, és biztosítani kell a bizalmasságát[14], sértetlenségét[15] és rendelkezésre állását[16]. [7][10]

A MINŐSÍTETT ADATOK VÉDELMÉRŐL SZÓLÓ 2009. ÉVI CLV. TÖRVÉNY LÉTREJÖTTÉNEK OKAI

A Sólyom László Köztársasági Elnök Úr és a Dr. Katona Béla Úr az Országgyűlés elnöke által aláírt, a minősített adat védelméről szóló törvényt, mely 2010. április 1.-jén lépett hatályba, alapvetően az állami és közfeladatok zökkenőmentes, zavartalan biztosítása érdekében, a közérdekű adatok megismerésének alkotmányos jogából, valamint ennek a jognak a kizárólag szükséges és arányos mértékű korlátozásából kiindulva alkotta meg az Országgyűlés. A törvény megalkotása időszerű volt több szempontból is, értendő ez alatt az idejétmúlt korábbi szabályozás aktualizálása, egyértelművé tétele, a hiányzó szabályozási részelemek, részterületek, a minősített adatok kezelésével foglalkozó nélkülözhetetlen új intézmények, szervezeti elemek felállítása, létalapjuk és intézményrendszerük megteremtése, a hazai szabályozásnak a szövetségesi rendszerekben működő szabályozásnak és gyakorlatnak való megfeleltetése.

Ennek az új törvénynek a megalkotását az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény szükségessé vált átfogó felülvizsgálata során feltárt hiányosságok tették indokolttá. A felülvizsgálat alkalmával megállapítást nyert többek között, hogy kifejezetten sok a „Szigorúan titkos" és a „Titkos" minősítési jelzéssel ellátott nemzeti minősített adat. Ugyanakkor problémát jelentett bizonyos jogintézmények hiánya is, mint a nemzeti személyi és telephely biztonsági tanúsítványok és a nemzeti iparbiztonsági rendszer, melynek következtében például EU Telephely Biztonsági Tanúsítvány hiányában magyar gazdálkodó szervezetek nem vehettek részt az EU adatok megismerését indokolttá tevő tenderekben. Továbbá a különböző nemzetközi szervezetekben történő szerepvállalásunk, az Euroatlanti régióban elfoglalt helyünk is újabb problémákat, végrehajtandó feladatokat, és megoldásra váró szabályozási kérdéseket vetett fel ezen a téren. Ennek következtében a revízió rávilágított a külföldi, elsősorban NATO és EU, valamint a nemzeti minősített adatok védelmére vonatkozó követelményrendszerek közötti markáns különbözőségekre, mint például az elektronikus információbiztonságra[17] vonatkozó szabályok hiányára, a nemzetközi

---

rendszeresített számítógépek (palmtopok, laptopok, törzsmunkaállomások, digitálisan vezérlet híradó eszközök, ellenőrző és felderítő eszközök, fegyverek és fegyverrendszerek, stb.) kezelésének mesterfokú elsajátítása.

13 Információs harcos: „Az információs hadszíntéren az információs műveleti terv szerint digitális adatszerző, feldolgozó, továbbító, valamint támadó és védő információs műveleti eszközökkel (fegyverekkel), eljárásokkal harcolnak."

14 Bizalmasság: A minősített adatot csak az arra jogosult személy ismerheti meg, csak ő férhet hozzá. Nem fordulhat elő illetéktelen, jogosulatlan információszerzés vagy a minősített adat nyilvánosságra kerülése.

15 Sértetlenség: A minősített adat tartalmát csak az arra jogosult személy változtathatja meg, illetve az adatot csak ő törölheti. Kiküszöböli annak a lehetőségét, hogy a minősített adatot észrevétlenül módosítsák.

16 Rendelkezésre állás: Lehetővé teszi, hogy az arra jogosult személy számára a minősített adat elérhető, hozzáférhető legyen, egyáltalán, hogy használni tudja azt.

17 Elektronikus információbiztonság: INFOSEC – Information security (Electronic information security). „A távközlési és informatikai, valamint egyéb elektronikus rendszerekben és támogató infrastruktúráiban alkalmazott

szervezetek minősített adatok kezelésére vonatkozó szabályrendszereiben bekövetkezett változások (EU) hazai szabályozásba való integrációjának, átültetésének elmaradására. Az új titokvédelmi törvény hiányában jelentős nehézségekbe ütközött többek között a minősített adatok cseréjével járó két vagy többoldalú biztonsági megállapodások megkötése is, nem volt megfeleltetés a nemzetközi szervezetek gyakorlatában alkalmazott és a nemzeti minősítési szintek vonatkozásában, valamint a Bűntető Törvénykönyv állam és szolgálati titok megsértésére vonatkozó paragrafusai ugyancsak nem álltak összhangban a NATO szabályozással. [7][13][[14]

ALAPVETŐ CÉLOK

A törvény megalkotásával alapvető célul tűzték ki többek között a jogállamiság intézményének alappillérét megtestesítő alapvető jogok tiszteletben tartása, az ország érdekeinek védelme és a nemzetközi kötelezettségvállalásainak maradéktalan teljesítése érdekében, a minősített adatok létrejöttével, kezelésével, a minősítési eljárással, a nemzeti minősített adatok felülvizsgálatával kapcsolatos rendszabályok, a minősített adatok védelme általános szabályainak, az ezt megvalósító személyek és szervezetek körének, a nemzeti iparbiztonsági rendszer főbb eleminek a meghatározását. Szükségessé vált tehát egy egységes követelményrendszer megfogalmazása mind a nemzeti mind a külföldi minősített adatok védelmével kapcsolatban. A törvény megalkotásának indokai között felvonultatott probléma okán, mely a nagyszámú nemzeti minősített adat létére utal, egyértelműen következik, hogy a törvényalkotás egyik alapvető célját testesítette meg ezen adatok volumenének a redukálása. Célként fogalmazható meg többek között a széttagolt szakmai felügyeleti rendszer egységesítése is. [7]

A törvényalkotó természetesen alapul vette a minősített adat kezelésére vonatkozó alapvető kritériumokat, mint a bizalmasság, a sértetlenség és a rendelkezésre állás elvét párhuzamban a szükségesség és arányosság[18], valamint a szükséges ismeret[19] elvének figyelembevételével. [7][10]

ÉRTELMEZŐ RENDELKEZÉSEK

Mint a törvények nagy többségében, és mint az a korábbi 1995. évi LXV. az államtitokról és szolgálati titokról szóló törvényben is tapasztalható volt, ebben az esetben is sor került az egységes értelmezéshez, közös nyelvezethez elengedhetetlenül szükséges fogalomcsokor meghatározására és kifejtésére. Ennek keretében a törvény vonatkozó paragrafusa és annak alpontjai magukba foglalják a minősített adat és az ahhoz szorosan kapcsolódó fogalomtár definiálását, egységes keretbe integrálva a minősített adat kezeléséhez fűződő eljárásokkal, személyekkel, szervezetekkel kapcsolatos definíciókat.

Az információs társdalom „elektronikus íróasztalán” egymás mellé fektetvén a korábbi törvényt és annak utódját, első látásra szembeötlővé válik az a nagyon fontos észrevétel, hogy az aktuális passzus szól, illetve rendelkezik a megértés alapját képező olyan új definíciókról, mint a személyi biztonsági tanúsítványról[20], a telephely biztonsági

rendszabályok összessége amelyek védelmet nyújtanak az előállított, feldolgozott, tárolt, továbbított és megjelenített információk, bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen.

18 Szükségesség és arányosság elve: A közérdekű adatok nyilvánosságának korlátozásával foglalkozik, melynek értelmében az adat nyilvánossághoz fűződő jogát csak a törvényi feltételek teljesülése esetén, a védelméhez szükséges mértékű minősítési szinttel és csak a feltétlenül szükséges ideig lehet korlátozni.

19 Szükséges ismeret elve: Az elv a minősített adat megismeréséről rendelkezik, melyet azon személyek részére tesz lehetővé, akiknek az állami vagy közfeladataik ellátásához feltétlenül szükséges.

20 Személyi biztonsági tanúsítvány: A 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „az a tanúsítvány, amely érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kaphat felhasználási engedélyt.”

tanúsítványról[21], és az elektronikus adatkezelő rendszerről[22], mely fogalmak törvényi meghatározása, leszabályozása kvázi az új törvény megalkotása indokainak tárházában jelesen képviseltetik magukat, mint azt korábban említettük volt. Véleményem szerint megemlítendő jelentős különbözősége az értelmező rendelkezéseknek az is, hogy a titokbirtokos[23] fogalmát szétbontva az új törvény vonatkozó paragrafusai különbséget tesznek a minősítő[24], a felhasználó[25] és a közreműködő személye[26] között is. [7][14]

A MINŐSÍTŐK ÉS A MINŐSÍTÉSI ELJÁRÁS SZABÁLYAI

A törvény vonatkozó paragrafusa szabályozza, és egyértelműen meghatározza azon személyek körét, akik feladat és hatáskörükben egy adat vonatkozásában minősítő jogkörrel rendelkeznek. Ezzel párhuzamosan szabályozza magát a minősítés tevékenységét is, beleértve a minősítéssel védhető közérdekek körének meghatározását, az adat minősítésének egyes eseteit, az alkalmazható minősítési szintek megjelölését és a nemzeti minősített adat felülvizsgálatának és felülbírálatának egyes eseteit.

Itt fontos megemlítenünk a törvény hordozta legjelentősebb változások közül néhányat, melyeket a fent nevezett cím alatt csoportosuló vonatkozó paragrafusok hordoznak magukban. Egyik ilyen változás, hogy a minősítők körében a Legfelsőbb Bíróság elnöke mellett az Országgyűlés Igazságszolgáltatási Tanácsának az elnökét is megjeleníti, ebbe a körbe sorolja továbbá a Nemzeti Biztonsági Felügyelet vezetőjét is, ugyanakkor olyan, az 1995. évi LXV. törvényben meghatározott személyek, mint az Országos Egészségbiztosítási Pénztár elnöke vagy az Országos Nyugdíjbiztosítási Főigazgatóság főigazgatója, a jelen törvényben nem kerülnek a minősítők körébe sorolásra.

Ugyancsak markáns eltérés a két törvény között, hogy az utóbbi esetében az egyes minősítési szinteket az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által okozható kár mértéke határozza meg. Ennek megfelelően „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" minősítési szintekről szól, mely szintek már teljes harmóniát mutatnak többek között a NATO-ban alkalmazott minősítési szintekkel[27]. Ugyanakkor ennek folyamodványaként megszűnik az „Államtitok" és „Szolgálati" titok, mint minősítési szint kategória, melyről a korábbi törvény még aktívan rendelkezett, és ezzel egyetemben módosításra kerültek a különböző minősítési szintek érvényességi ideje is. Az 1995. évi LXV. törvény értelmében az akkor megfogalmazott „Államtitok" kategória maximális érvényességi idejét 90 évben, a „Szolgálati titok" kategória érvényességi idejét, pedig 20 évben limitálta a törvényalkotó. Jelen esetben ez oly módon változott meg, hogy a „Szigorúan titkos" és „Titkos" minősítési szint esetén 30 évben, a „Bizalmas" minősítéssel ellátott adat esetén 20 évben, a „Korlátozott

21 Telephely biztonsági tanúsítvány: A 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „az a tanúsítvány, amely meghatározza, hogy a gazdálkodó szervezet milyen legmagasabb minősítésű szintű minősített adat kezelésére alkalmas".

22 Elektronikus rendszer: Az elektronikus adatkezelő rendszer a 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „minősített adat elektronikus, elektromagnetikus vagy optikai úton történő kezelésére alkalmas berendezés, módszer és eljárás együttese".

23 Titokbirtokos: Az 1995. évi LXV. törvény általános rendelkezések értelmében „a minősítő, valamint az a személy vagy szerv, akinek vagy amelynek a minősített adatot … továbbították".

24 Minősítő: A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „feladat és hatáskörében minősítésre jogosult személy".

25 Felhasználó: A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „az a személy, akinek állami vagy közfeladat végrehajtása céljából a felhasználói engedély kiadására jogosult vezető a minősített adatra vonatkozóan a felhasználói engedélyben rendelkezési jogosultságokat biztosít".

26 Közreműködő személy: A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „az a természetes személy, aki az állami vagy közfeladatot ellátó szerv feladat- és hatáskörébe tartozó ügyben segítséget nyújt, és ehhez minősített adat felhasználása is szükséges."

27 NATO-ban alkalmazott minősítési szintek: „NATO Cosmic Top Secret", „NATO Top Secret", „NATO Confidential", „NATO Restricted"

terjesztésű" minősítési szinttel védett adat esetén, pedig legfeljebb 10 évben állapította meg az érvényesség idejét a törvényalkotó. Természetesen meghatározott módon, korlátozott formában, de mind a két törvény lehetőséget biztosított és biztosít a különböző minősítési szintek érvényességi idejének a meghosszabbítására. Továbbá az új törvény azonosítja az új minősítési szinteknek megfelelő típusú nemzetbiztonsági ellenőrzések szintjét is, mely „Szigorúan titkos" minősítés esetén „C", „Titkos" minősítés esetén „B", „Bizalmas" minősítés esetén „A" típusú nemzetbiztonsági átvilágítást követel meg. A „Korlátozott terjesztésű" minősítési szint esetén a törvény nem rendelkezik nemzetbiztonsági kérdőív kitöltéséről. [7][14]

KÜLFÖLDI MINŐSÍTETT ADAT

A 2009. évi CLV. törvény vonatkozó paragrafusai kifejezetten a külföldi minősített adatok kezelésére helyezik a hangsúlyt, melyre a korábbi törvényben nem történt intézkedés.

A 2009. évi törvény a 2. számú mellékletében összefoglalja, rendszerezi a különböző nemzetközi szervezetek, mint a NATO, EU, NYEU, EURATOM[28], EUROPOL[29], EUROJUST[30] által alkalmazott minősítési szinteket, és azonosítja az ezeknek megfelelő nemzeti minősítési szinteket. Ha visszagondolunk a korábban említett, a törvény megalkotását szorgalmazó indokokra, célokra, a nemzeti és külföldi minősített adatok jelölésére szolgáló, a hazai és nemzetközi szervezetek gyakorlatában alkalmazott egyes minősítési szintek egymáshoz illesztése, egymásnak való megfeleltetése, harmonizációja ugyancsak időszerű és halasztást nem tűrő ok volt.

Nagyon fontos kiemelni, hogy a törvény rendelkezése értelmében, abban az esetben, ha a nemzeti minősített adat külföldi minősített adatot is tartalmaz, akkor annak minősítési szintje és a minősítés érvényességi ideje nem lehet kisebb és rövidebb, mint a külföldi minősített adat minősítési szintje és annak érvényességi ideje. [7][14]

A MINŐSÍTETT ADAT BIZTONSÁGÁRA VONATKOZÓ SZABÁLYOK

A minősített adatok védelméről szóló törvény a minősített adatok biztonságára vonatkozó szabályok részének első, 10 §-a egy jelentős kritériumot fogalmaz meg a minősített adatok kezelésével kapcsolatban, melynek értelmében minősített adatot kezelni csak a Nemzeti Biztonsági Felügyelet által kiadott engedély alapján lehet, mely szerv új elemként jelent meg korábban a törvénynek a minősítők körét meghatározó paragrafusa alatt. Ezt megelőzően az államtitokról és szolgálati titokról szóló törvény vonatkozó rendelkezése a belügyminiszter felügyeleti jogkörének keretébe helyezte a minősített adatok védelmének szakmai felügyeletét.

A minősített adatokhoz való hozzáférést kizárólagosan a személyi biztonsági tanúsítvány és titoktartási nyilatkozat meglétéhez köti. A személyi biztonsági tanúsítvány kiadása a Nemzeti Biztonsági Felügyelet hatáskörébe tartozó feladat. A minősített adat megismerésével kapcsolatban továbbra is megmarad a megismerési engedély és titoktartási

28 EURATOM: The European Atomic Energy Community - Európai Atomenergia Közösség. Egy nemzetközi szervezet, melyet 1957.-ben alapítottak a második római szerződéssel. A közösség lényege abban áll, hogy a szerződés aláírói egyértelmű szándékukat fejezték ki az atomenergia békés célú felhasználásával kapcsolatban és az atomenergia-iparban történő készséges együttműködésük iránt. Több ügynöksége létezik, többek között Spanyolországban.

29 EUROPOL: The European Police Office - Európai Rendőrségi Hivatal. Az Európai Unió rendvédelmi ügynöksége, melynek legfontosabb célkitűzése egy biztonságosabb Európa megteremtése, segítségnyújtás az Európai Unió tagállamai rendvédelmi szervei részére a nemzetközi bűnözés és terrorizmus visszaszorítása érdekében. Székhelye Hollandia.

30 EUROJUST: The European Union's Judicial Cooperation Unit - Európai Igazságügyi Együttműködési Egység. A szervezet 2002-ben lett létrehozva az EU által azzal a céllal, hogy előmozdítsák az együttműködést az uniós tagállamok igazságügyi hatóságai között a két vagy több uniós tagállamot érintő nyomozati és büntetőeljárások keretében. Székhelye Hollandia.

nyilatkozat intézménye mondhatni a személyi biztonsági tanúsítvány intézményén belül, leszabályozva azokat az eseteket a megismeréssel és felhasználással kapcsolatosan, amikor az érintettnek nem kell rendelkeznie a nevezett tanúsítvánnyal.

Továbbá előírja, hogy minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a személyi[31], fizikai[32], adminisztratív[33] és elektronikus biztonság [10] feltételeket is. Ez önmagában véve nem jelentene merőben új szabályozást, hiszen az előző törvény a titokbirtokos szerv vezetőjének feladat és hatásköre keretében rendelkezik a minősített adatok védelmi rendszerének biztonsági elemeiről, beleértve az imént felvázolt biztonsági feltételeket is, de az új törvény már külön rendelkezik az elektronikus rendszereken kezelt minősített adat és az elektronikus rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának kérdésében is, melyről az 1995. évi LXV. törvényben még nem találunk említést.

Ugyancsak új rendelkezése a törvénynek a személyi biztonsági tanúsítvány intézménye mellett a telephely biztonsági tanúsítvány intézménye is a gazdálkodó szervezetek vonatkozásában, melynek kibocsátását a Nemzeti Biztonsági Felügyelet hatáskörébe utalja. A telephely biztonsági tanúsítvány kibocsátása az iparbiztonsági ellenőrzés lefolytatását követően válik indokolttá abban az esetben, - természetesen, ha kockázati tényezők nem merülnek fel - amikor a minősített adatot kezelő szervnek az állami vagy közfeladata ellátása érdekében gazdálkodó szervezet közreműködését veszi igénybe. [7][13][[14]

A MINŐSÍTETT ADAT VÉDELMÉT ELLÁTÓ SZERVEZETEK ÉS SZEMÉLYEK

A 2009. évi CLV. törvény soron következő V. nagy fejezetében kerülnek meghatározásra a minősített adatok kezelésével kapcsolatban érintett személyek és szervezetek, többek között a már oly sokat emlegetett Nemzeti Biztonsági Felügyelet is. A törvény részletekbe menően szabályozza az érintett szervezet tevékenységi körét, legfőbb feladatát, mely többek között nem más, mint a minősített adat védelmének hatósági felügyelete, a minősített adat kezelésének hatósági engedélyezése és felügyelete, továbbá a nemzeti iparbiztonsági hatósági feladatok ellátása. Korábban az 1995. évi LXV. az államtitokról és szolgálati titokról szóló törvény értelmében a titokbirtokos szerv vezetőjének hatás és feladatkörébe tartozó tevékenység volt a minősített adatok védelméről szóló jogszabályok végrehajtásáról, illetve a hatáskörében keletkezett vagy más szervek által átadott minősített adatok védelmi rendszerének különböző biztonsági elemekkel való kiépítettségéről és működtetéséről történő gondoskodás, mint azt korábban említettük volt.

A felügyelet feladat és tevékenységi körének legfontosabb részét képezi az új törvény által életre hívott személyi biztonsági tanúsítvány, telephely biztonsági tanúsítvány kiadása, a minősített adatok kezelésére szolgáló elektronikus rendszerek használatbavételének engedélyezése, a rejtjeltevékenység hatósági engedélyezésének és felügyeletének biztosítása, a minősített adatok védelmével kapcsolatos bejelentések kivizsgálása, csakhogy néhányat említsünk a legfontosabbak közül. Továbbá korábban említettük volt, hogy az új törvény megalkotásának egyik fontos indokaként jelenik meg a nemzetközi szervezetekkel, szabályozással való harmonizáció, ebből kifolyólag a törvényalkotó a felügyelet

31 Személyi biztonság: „…a minősített információ csak olyan személynek juthat birtokába, aki megfelelő szintű személyi biztonsági követelményeknek igazoltan megfelel, illetve az adott minősítésű információ megismerése számára hivatalos célból szükséges. A személyi biztonság megteremtésének egyik legfontosabb eljárása a nemzetbiztonsági ellenőrzés."

32 Fizikai biztonság: „Azon rendszabályok és tényleges akadályok - …falak,…behatolás jelzők, beléptető rendszerek, stb. – összessége, melyek megfosztják az illetékteleneket a minősített, kritikus információkhoz, dokumentumokhoz, eszközökhöz való hozzáféréstől… és meghiúsítják vagy megakadályozzák a fizikai támadást."

33 Dokumentumbiztonság: „ A titokvédelem tágabb értelmezése, amely azt jelenti, hogy az összes dokumentumot a minősítésének, az érzékenységének, vagyis a titkossági osztályba sorolásának megfelelően kell védeni….A dokumentumbiztonság közvetlenül kapcsolódik az elektronikus információbiztonsághoz, hiszen valamennyi elektronikus adathordozó egyben dokumentumnak is minősül."

tevékenységi körébe utalta a különböző nemzetközi szervezetek vonatkozó szabályzataiban, illetve a minősített adatok védelme tárgyában kötött nemzetközi szerződésekben a nemzeti biztonsági hatóságok számára előírt feladatok ellátását is. [7][14]

MÓDOSULÓ RENDELKEZÉSEK

Mivel a 2009. évi CLV. törvény a minősített adatok védelméről jelentős változást hoz a korábbi 1995. évi LXV. törvény az államtitokról és szolgálati titokról törvény vonatkozásban, ha már csak az új megnevezésekre, tanúsítványokra vagy szervezetekre gondolunk is, ezért elengedhetetlenül szükséges mindazon releváns törvényekről és az őket kő keményen érintő módosító rendelkezésekről megemlékezni, melyeket maradéktalanul harmonizálni szükséges az új törvény tükrében. Részletekbe menően nem kívánunk kitérni e módosító rendelkezések hosszas felsorolására, csupán címszavakban kívánjuk megemlíteni az érintett törvényeket.

A 2009. évi törvény alkotta szabályozás szorosan érinti tehát többek között a „Büntető Törvénykönyvről szóló 1978. évi IV. törvény", „A csődeljárásról és felszámolási eljárásról szóló 1991. évi XLIX. törvény", „Az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény", „A szervezett bűnözés, valamint az azzal összefüggő egyes jelenségek elleni fellépés szabályairól és az ehhez kapcsolódó törvénymódosításokról szóló 1999. évi LXXV. törvény", „Az elektronikus hírközlésről szóló 2003. évi C. törvény", „Az Európai Parlament magyarországi képviselőinek jogállásáról szóló 2004. évi LVII. törvény", „A légi-, a vasúti és a vízi-közlekedési balesetek és egyéb közlekedési események szakmai vizsgálatáról szóló 2005. évi CLXXXIV. törvény", „Az elektronikus közszolgáltatásokról szóló 2009. évi LX. törvény", „Az országgyűlési képviselők jogállásáról szóló 1990. évi LV. törvény", „A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény", „Az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény", „A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény", valamint „A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény" releváns paragrafusait. [7][14]

FELHATALMAZÁS

A törvényalkotó felhatalmazza a Kormányt, hogy rendelettel szabályozza a törvényben megjelenő, a korábbi törvényhez képest végbemenő legfontosabb változásokat, értendő ezalatt, hogy a Kormány állapítsa meg többek között a Nemzeti Biztonsági Felügyelet részletes feladatait, eljárás és működési rendjét, a minősített adatok kezelésének rendjét, a minősített adat elektronikus kezelésének részletes szabályait, a rejtjeltevékenység engedélyezésének rendjét és a hatósági felügyeletének részletes szabályait, valamint az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályait. [7]

ZÁRÓ RENDELKEZÉSEK

A jogharmonizáció elősegítése érdekében a 2009. évi CLV. törvény a záró fejezetében rendelkezik a két törvény közötti átmeneti időszakban végrehajtandó intézkedésekről, elindított folyamatokról és határidőkről, megszűnő törvényekről és újabb, esetenként minősített többséget igénylő módosító rendelkezésekről is úgy, mint a személyi biztonsági tanúsítvány beszerzésének, a minősített adatok védelmére vonatkozó fizikai és elektronikus biztonsági feltételek megteremtésének a határidejéről, az 1995. évi LXV. törvény az államtitokról és a szolgálati titokról hatályát vesztéséről, és olyan már korábban is említett

esetekről, melyek az új törvény megszületése és hatályba lépése következtében módosulásokon kell, hogy átessenek. [7][14]

REZÜMÉ

Összegezvén a minősített adatok védelméről szóló 2009. évi CLV. törvény legfontosabb passzusait, dióhéjban az alábbi gondolatokat kell felelevenítenünk. Leszögezhetjük, hogy a törvény megalkotása a korábbi szabályozás hiányossága, idejétmúlt volta, a nemzetközi szabályozásban végbemenő változások, a szabályozási rendszerek és törvényi hátterek harmonizációjának szükségessége okán indokolt volt. Olyan új változások következtek be, mint például a különböző minősítési szinteknek az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által okozható kár mértéke által történő meghatározása, az „Államtitok" és „Szolgáti titok" minősítési szintek megszűntetése, a „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" minősítési szintek meghatározása, az egyes szintek maximális érvényességi idejének újralimitálása, a hozzájuk szükséges nemzetbiztonsági átvizsgálási szintek újradefiniálása, a Nemzeti Biztonsági Felügyelet felállítása, hatás, feladat és tevékenységi körének meghatározása, a személyi és telephely biztonsági tanúsítvány fogalmi kategória megalkotása, az elektronikus információbiztonságra vonatkozó szabályok életre hívása, az iparbiztonsági ellenőrzés intézményének megteremtése, csakhogy a legfontosabbakat említsük a teljesség igénye nélkül.

HIVATKOZÁSOK

[1] „Zöld Könyv" A távközlési, média és információ-technológiai szektorok konvergenciájáról és ennek szabályozási kihatásairól. European Comission, Brüsszel, 1997. december 03. (Forrás: http://www.itb.hu/dokumentumok/zold_konyv/index.html#toc /letöltés ideje: 2009.11.10./)

[2] Jobbágy Szabolcs: Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő. – In: Hadmérnök A ZMNE Bolyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On - line Tudományos Kiadványa, 2009. március, IV. évfolyam 1. szám (elektronikus) – p. 184-196. (Forrás: http://www.hadmernok.hu/2009_1_jobbagy.pdf /letöltés ideje: 2009.11.10./)

[3] Magyar Hadtudományi Társaság: Hadtudományi Lexikon I. kötet. Szabó József (főszerk.) – Budapest, 1995 – ISBN 963 04 5227 8

[4] Dr. habil Sándor Miklós nyá. ezds – Farkas Tibor fhdgy. – Jobbágy Szabolcs fhdgy.: Híradásszervezés jegyzet a BJKMK Híradó Tanszék BSc, MSc és PhD hallgatói számára – Budapest, ZMNE EEK, 2009 – 109 p.

[5] Muha Lajos: Infokommunikációs biztonsági stratégia. – In: Hadmérnök A ZMNE Bolyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On - line Tudományos Kiadványa, 2009. március, IV. évfolyam 1. szám (elektronikus) – p. 214-224. (Forrás: http://hadmernok.hu/2009_1_muha.pdf - /letöltés ideje: 2009.11.14./)

[6] Magyar Honvédség Öszhaderőnemi Doktrína 3. kiadás (ÁLT/27) – Honvédelmi Minisztérium kiadványa, 2010.

[7] 2009. évi CLV. törvény a minősített adat védelméről – Magyar Közlöny a Magyar Köztársaság Hivatalos Lapja, 2009. december 29. kedd, 194. szám (Forrás: www.nbf.hu/anyagok/jogszabaly/09CLV.doc - /Letöltés ideje: 2010.04.14./)

[8] Dr. Seres György: A digitális hadszíntér határai. – Előadás a Robothadviselés I Konferencián (elektronikus változat), 2001 – 11 p. (Forrás: http://drseres.com/publik/pdf/digit_hun.pdf - /letöltés ideje: 2010.04.06./)

[9] Gácser Zoltán mk. őrgy.: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben. – Doktori PhD értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2008.

[10] Dr. Haig Zsolt mk. alez.: Az információs társadalom információbiztonsága Egyetemi jegyzet. – Budapest, ZMNE EKK, 2009 – 179 p.

[11] Nagy Zoltán: A 21. század fegyveres küzdelmeinek irányai és kihívásai a NATO szemszögéből. –In: Hadtudomány. A Magyar Hadtudományi Társaság folyóirata, 2005. december, XV. Évfolyam, 4. szám (elektronikus) (Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_4.html /letöltés ideje: 2010.04.06./)

[12] Várhegyi István – Makkay Imre. Információs korszak, információs háború, biztonságkultúra. – Budapest, OMIKK, 2000 – 296 p. – ISBN 963593 238-3

[13] Zala Mihály: Az új információvédelmi törvény és kihatásai. – Innovációval a Védelemért és a Biztonságért Társaság Innovációs Klub klubnapján elhangzott előadás anyaga, 2010. január 20. (Forrás: http://www.ivb.org.hu/IC-Download.php - /letöltés ideje: 2010.04.17./)

[14] 1995. évi LXV. törvény az államtitokról és a szolgálati titokról – A Magyar Köztársaság Információs Hivatala – (Forrás: http://www.mkih.hu/torvenyek/t9500065/t9500065.htm#kagy1 /letöltés ideje: 2010.04.21./)

Kassai Károly
kassai.karoly@hm.gov.hu

A BIZTONSÁGOS ELEKTRONIKUS ADATKEZELÉSHEZ SZÜKSÉGES FIZIKAI VÉDELEMRE ÉS ÜZEMELTETÉSI KÖRNYEZETRE VONATKOZÓ ÁLTALÁNOS KÖVETELMÉNYEK

Absztakt

A hatékony fizikai hozzáférési rendszabályok és a megfelelően kialakított környezeti elemek és támogatás fontos szempontja a biztonságos elektronikus adatkezelésnek.
Általánosságban beszélve mindenki tudja és érti a fizikai védelmi rendszabályok fontosságát, de a gyakorlati életben ez a terület számtalan esetben hiányosságokat, félreértéseket tartalmaz. A cikk a híradó és informatikai rendszerek (CIS) jobb támogatása érdekében azonosítja a legfontosabb részeit a biztonság e területének és általános szabályokat, egyszerű példákat ad.

The effective physical access control and the appropriately implemented environmental elements and support are important dimensions of the secure electronic information handling.
Generally speaking everybody knows and understands the importance of physical measures but in real life these issues contain some gaps and misunderstandings.
This article identifies the key factors of this security field and gives some general rules and simple examples for the better support of CIS.

Kulcsszavak: *információbiztonság/információvédelem, fizikai biztonság, hozzáférés felügyelet, üzemeltetési biztonság ~ information security, physical security, access control, operating security*

BEVEZETÉS

Az elektronikus adatkezelő rendszerek, eszközök telepítése és üzemeltetése során megkerülhetetlen kérdés az üzemeltetési környezet szabályozása, illetve általánosságban olyan környezet kialakítása, amely rendszer-specifikusan, kifejezetten az adott elektronikus adatkezelésre szabottan biztosítja az eszközök működését, a munkavégzést, illetve szükséges esetben lehetővé teszi az igényeknek megfelelően a cserét, fejlesztést vagy a javítást, karbantartást.

Ez a terület jogszabályokban összefogottan nem szabályozott, csak a fizikai biztonság egyes területeire találhatók követelmények, főleg a minősített adatkezelésre vonatkozóan [1]. A nemzetközi szabványok [2] alapján kialakított nemzeti ajánlás [4] tekinthető az első olyan nemzeti szabályozási alapnak, mely elkezdte a kérdés rendezését.

A honvédelmi tárcánál ehhez hasonlóan egyes rendszerekhez, tevékenységekhez rendelt rendszabályok lelhetők fel, korszerű biztonsági szempontok által vezérelt átfogó szabályozás nem azonosítható.

A szabványok, jogszabályok, a nemzeti ajánlás, illetve az adatkezelésre vonatkozó NATO, EU követelmények alapján e szakkérdések szabályozását három szinten célszerű kialakítani: a biztonságpolitikában-, a tárca szintű általános követelményekben, és a rendszer-specifikus biztonsági dokumentumokban [5].

E cikk a *tárca szintű szabályozás* azon kulcskérdéseit célozza, melyek minősített adatok érintése nélkül még tárgyalhatók, és *elég támpontot adnak az üzemeltetési környezet kialakításában és fenntartásában érintetteknek*. Ennek megfelelően szabályozási cél:

- technikai megoldások alkalmazásával és a fizikai elérésre vonatkozó eljárásrend bevezetésével és fenntartásával az elektronikus adatkezelő rendszerek biztonságos környezetének kialakítása, ahol a védelmi rendszabályok kockázat- és értékarányosan fenntarthatók;
- az elektronikus adatkezelő rendszerek, eszközök megfelelő üzemeltetési környezetének biztosítása.

1. ÁLTALÁNOS KÖVETELMÉNYEK

A felhasználói irodákban, helyiségekben, valamint a központi kiszolgálást biztosító helyiségeknél az adatok és adatkezelő eszközök biztonsága érdekében *a biztonsági besorolásnak, a kezelt adatok mennyiségének, az adatkezelés sajátosságainak* a jogszabályokban meghatározott követelményeknek megfelelő, kockázatokkal arányos fizikai védelmi rendszabályokat kell alkalmazni.

A védelmet *ki kell terjeszteni az elektronikus adatkezelő rendszer üzemeltetése szempontjából kritikus létesítményekre is*, mint rendezők, áramellátást biztosító helyiségek, anyagraktárak, szoftverek és rendszerdokumentációk tárolására szolgáló helyiségek. Ebből következik, hogy *az adatkezelő eszközöket funkciójuknak megfelelően kell csoportosítani* és ennek megfelelően az adatkezelő helyiségeket azonos védelmi zónákban kell elhelyezni. Az üzemeltetéshez, felügyelethez szükséges *hozzáférési jogosultságokat csak a munkavégzéshez szükséges zónákhoz, helyiségekhez szabad biztosítani*.

Napjainkban – szerencsére – egyre jobban *előtérbe kerül a hálózatokban történő gondolkodás,* illetve a *felhasználói igények központi kiszolgálására vonatkozó szándék*. Ez lassan, de biztosan elmossa az „én szervertermem” típusú szervezeti gondolkodást és egyben utat nyit a költséghatékony – és egyben biztonságosabb – centralizált megoldások felé. Lehetővé válik a központi kiszolgálás megalapozása, az erőforrások koncentrálása, a korábban gyakran tapasztalt kevésbé hatékony megoldások helyett. Az országos hálózathoz történő csatlakozást nem szükséges katonai szervezetenként (akár azonos épületben is) kialakítani, vagy szervezetenként elkülönített hálózati kiszolgálókat egymástól függetlenül üzemeltetni.

A különböző szintű fizikai védelemmel ellátott zónák közötti mozgást ellenőrizni kell, és a mozgásra vonatkozó adatokat a szervezeti követelményeknek megfelelően rögzíteni és meghatározott ideig tárolni kell.

Az alap biztonság osztályú adatok kezelésére feljogosított elektronikus adatkezelő rendszerek fizikai védelmét az MH Egységes Iratkezelési Szabályzat általános követelményei alapján, a rendszer-specifikus biztonsági követelmények figyelembe vételével kell kialakítani.

A fokozott biztonsági osztályú adatok kezelésére feljogosított elektronikus adatkezelő rendszerek fizikai védelmét a kockázatelemzés alapján meghatározott rendszabályokkal kell megerősíteni. A rendszer felépítésétől függően a hálózati erőforrásokat, rendszerelemeket biztonsági területen kell elhelyezni.

A nemzeti, NATO, EU KORLÁTOZOTT TERJESZTÉSŰ minősítéssel rendelkező adatkezelő eszközöket a vonatkozó jogszabályban meghatározott követelmények szerint kialakított biztonsági területen, vagy adminisztratív zónában kell elhelyezni. A nemzetközi megállapodás alapján átvett külföldi minősített adat védelmére a vonatkozó jogszabály szerinti védelmi rendszabályokat kell alkalmazni, *kiegészítve a nemzetközi megállapodásban rögzített specifikációkkal*.

A nemzeti, NATO, EU BIZALMAS, vagy magasabb minősítésű adatokra vonatkozó biztonsági osztályba tartozó elektronikus adatkezelő eszközöket a vonatkozó jogszabályban meghatározott követelményeknek megfelelően az alábbiak szerint kell elhelyezni:

- a központi hálózati elemeket I. osztályú biztonsági területen;
- a felhasználói munkaállomásokat I. vagy II. osztályú biztonsági területen.

A biztonsági területen belül rendszeres időközönként ellenőrizni kell a védelmi rendszabályok betartását, a látogatókkal kapcsolatban kontrollokat kell alkalmazni. Azon biztonsági területen, ahol rejtjeltevékenység folyik, *kiegészítő védelmi rendszabályokat kell alkalmazni* (a kiegészítő rendszabály *nem más, eltérő rendszabályt-, hanem a biztonság szintjének emelését jelenti*).

Gyakran feledett (vagy mellőzött) kérdés, hogy az I. vagy II. osztályú területre belépéskor és távozáskor szúrópróbaszerű ellenőrzéseket kell tartani az illetéktelen adatmozgás feltárása érdekében. Ebben az esetben a biztonsági területre történő belépéskor a belépők által látható helyre az ellenőrzésekre vonatkozó figyelmeztetést kell elhelyezni, a figyelmeztetésnek tartalmaznia kell, hogy a belépés feltétele az ellenőrzés. Egyértelműen tudatni kell a területen belül elvárt magatartást és belépéskor biztosítani kell a tiltott tárgyak eszközök látogatás alatti megőrzését. Biztonsági területre tiltani kell a magántulajdonú elektronikus adatkezelő eszközök bevitelét (amely szabály nem csak a látogatókra, hanem az ott dolgozókra is vonatkozik).

Korábban gyakran félreértelmezett kérdésnek számított, de a NATO, EU, illetve a nemzetközi megállapodás alapján átvett külföldi minősített adat, valamint nemzeti minősített adat egy helyiségen belül kezelhető, amennyiben az adatokra, adatkezelő eszközökre vagy folyamatokra vonatkozó követelmények ezt lehetővé teszik.

Eltérő biztonsági osztályba tartozó rendszerelemek, felhasználói eszközök elhelyezhetők közös helyiségben, amennyiben az adatkezelő funkciók ezt nem zárják ki, és a védelmi rendszabályok betarthatók. Az eltérő biztonsági osztályba tartozó eszközöket tartalmazó helyiség fizikai és személyi biztonságra vonatkozó rendszabályait a magasabb biztonsági osztályra vonatkozó követelmények szerint kell kialakítani.

Rejtjelző eszköz és egyéb adatkezeléshez szükséges eszköz (pl. szerver, hálózati elem) közösen csak akkor helyezhető el, ha a rejtjelző eszköz kezeléséhez és üzembenntartásához szükséges műveletek bizalmassága az egyéb eszközök üzemeltetése mellett biztosítható.

Biztonsági területek között minősített adatkezelésben résztvevő eszköz szállítása – amennyiben az lehetséges –, az adathordozó egységek, panelek eltávolításával történhet. Az eszközök sértetlensége érdekében a szállítás ideje alatt folyamatosan biztosítani kell az eszközök illetéktelen felbontás elleni védelmét.

Géptermek, rendezők, szervertermek és egyéb hálózati elemek üzemeltetésére szolgáló helyiségekben *csak a meghibásodások elhárítására, tesztelésre szolgáló munkahelyek alakíthatók ki*.

Amennyiben a szervezet feladatai külső ügyfelek rendszeres fogadását igénylik, az adatfeldolgozási helyszínektől elkülönítetten kialakított látogatói tereket (tárgyaló, fogadó helyiség) kell kialakítani, és oda csak a közös tevékenység biztosításához szükséges elektronikus adatkezelő eszközöket lehet telepíteni valamint szükség esetén:

- a látogatókról jegyzéket kell vezetni;
- a látogatásra szolgáló helyiségekben a más feladatokhoz szükséges adathordozókat el kell távolítani (pl. szervezetre jellemző kimutatások, diagramok, telefonkönyvek és kivonatok, felelős személyek elérhetőségi adatai), és a rendszabály érvényesülését időszakosan ellenőrizni kell.

A minősített elektronikus adatkezelés területén *egyértelmű fejlődésként könyvelhető el a minősített adatkezelés és a rejtjelzésre vonatkozó követelmények egy jogszabályban történő megjelenítése*, ami megalapozza a közös eljárások kialakítását (pl. akkreditálás), illetve *támogathatja a rejtjelző és egyéb kommunikációs eszközök közös területen történő kialakításának kultúráját*, a nemzeti és NATO (vagy EU) eszközök indokolatlan elkülönítésének felszámolása. A kompromittáló kisugárzás elleni védelmi követelmények költségei jótékonyan támogatják a központi erőforrások centralizált elhelyezését és menedzselését, mert a helyiségekre szabdalt védelem vagy speciális eszközök ára sokszorosára növeli a költségeket.

Rendszer szinten a vázolt elvek mellett gondolni kell *a tartalék helyszínekre, tartalék hálózati csatlakozási pontokra, vagy a helyreállítást támogató eszközök, programok vagy biztonsági mentések tárolására szolgáló létesítmények kialakítására és fenntartására, a kezelt adatok biztonsági osztályának megfelelő fizikai védelmi megoldásokkal biztosítva*.

A fentiek jól szemléltetik, hogy az üzemeltetési környezet kialakításánál alapvetően megalapozható a káosz, és hosszú távon kőbe véshető a rugalmatlan szabályozás és áttekinthetetlenség. *A javító és karbantartó helyiségek hiánya, illetve az üzemeltetési funkciók elkülönítése ellen ható szokások gyakran eredményeznek ellenőrizhetetlen helyszíneket, áttekinthetetlen folyamatokat*. Káros hatásként említhető még *a szervezeti elkülönülésre való törekvés*, amikor egy telephelyen több helyiségben történik meg szervertermek, géptermek kialakítása az ezzel járó többlet kiadásokkal együtt. Az elkülönülésre irányuló hatások főleg minősített adatkezelés esetén megnövelhetik a kialakítás és fenntartás költségeit, és *nem minden esetben mutatnak a felhasznált erőforrásokkal arányos előnyöket*. Ugyanígy problémás a felhasználói és az üzemeltetői szerepkörök tudatos összemosása (lásd: „eddig is így csináltuk"; „ő írta a programot"; „nincs informatikusunk" vagy „eddig is az ő irodájában volt a szerver") *ami bonyolultabb rendszer esetén biztos, hogy összeomlással fenyeget, csak a hatásban képzelhetők el variációk*.

2. AZ ÜZEMELTETÉSI FELTÉTELEK KIALAKÍTÁSÁRA VONATKOZÓ ÁLTALÁNOS KÖVETELMÉNYEK

Amennyiben az üzemeltetett adatkezelő eszközt tartalmazó épület (vagy helyiség) körül teljes biztonsági felügyeletű terület nem biztosítható, a kompromittáló kisugárzás elleni védelem határaként az épület (vagy az adatkezelő helyiség) méreteit kell figyelembe venni.

Az elektronikus adatkezelő helyszínek kialakításakor figyelembe kell venni, és ellensúlyozni kell azokat a mechanikus-, hőmérsékleti-, elektromágneses hatásokat, por és egyéb szennyeződéseket, amelyek negatívan befolyásolhatják az eszközök működését.

Az elektronikus adatkezelő rendszer központi erőforrásainak elhelyezésére szolgáló helyiségeket a környezettől elválasztottan kell kialakítani, ahová csak a munkavégzésre feljogosított személyek számára, és csak a szükséges helyiségekbe biztosítható állandó belépés, valamint:

- a helyiséget úgy kell elhelyezni, hogy felette és a határoló falfelületeken vizes blokkot tartalmazó helyiségrész ne legyen, nyomó- és ejtőcsövek, gázvezetékek ne haladjanak át;
- a helyiségekhez csak az üzemeltetéshez elengedhetetlenül szükséges közműhálózat csatlakozhat;
- a helyiségek nem használhatók az üzemeltető személyek irodáiként, vagy más célra (pl. raktár, öltöző, műhely);
- a helyiségek összes határoló felületét, nyílászáróit az alkalmazott minősítési szintnek megfelelő biztonsági követelmények szerint kell kialakítani (pl. rakodó és csomagoló területek, menekülő ajtók);

- a kiszolgáló helyiségekben csak az engedélyezett információs folyamathoz tartozó eszközök, valamint az üzemeltetéshez szükséges anyagok, szerszámok tarthatók;
- az ellenőrizhetőség érdekében a helyiségben található eszközökről, berendezési tárgyakról naprakész, hiteles nyilvántartást kell vezetni;
- nagyobb mennyiségű hálózati eszköz vagy eltérő feljogosítással rendelkező üzemeltető személyzet esetében az eszközöket zárható rack szekrényben kell elhelyezni;
- eszközök ki és bevitele csak az üzemeltetett rendszerért felelős vezető jóváhagyásával történhet;
- az eszközök javítására, karbantartására az adott technológia függvényében azonos fizikai védelemmel rendelkező külön helyiséget, vagy elkülönített részt kell kialakítani;
- a tartalék eszközöket, anyagokat, szerszámokat úgy kell elhelyezni, hogy az üzemeltetési területet ért katasztrófa esetén azok, megsemmisülése, sérülése elkerülhető legyen (más helyszín, biztonsági távolság, tároló stb.);
- a minősített adatok kezelésére szolgáló eszközöket elkülönítetten, a hozzáférést a szükséges mértékben szabályozottan kell tárolni.

Magántulajdonú elektronikus adatkezelő eszköz, vagy adattároló az elektronikus adatkezelő rendszer elhelyezésére szolgáló biztonsági területen belüli helyiségekbe nem vihető be. Más szervezet tulajdonában lévő elektronikus adatkezelő eszköz, vagy adattároló csak az *illetékes vezető jóváhagyásával, egyedi azonosítást biztosító jelzés és ellenőrzés után, célhoz kötötten* vihető be a helyiségbe. A szükséges munka elvégzése után az eszközt ellenőrzés után lehet a helyiségből kivinni.

Az érzékeny adatokat kezelő elektronikus adatkezelő eszközöket a munkahelyeken úgy kell elhelyezni, hogy csökkentjen a rálátásból adódó illetéktelen megismerés veszélye.

A szervertermekben és egyéb központi kiszolgáló elemeket tartalmazó helyiségekben, valamint a felhasználói eszközöket tartalmazó helyiségekben tiltani kell az étkezést, dohányzást, vagy az egyéb szennyezést, károkozást okozó tevékenységet.

A fejlesztésre, tesztelésekre, képzésre és gyakorlásra szolgáló rendszerek, eszközök számára fizikailag elkülönített helyiségeket kell kialakítani. *A rendszerek üzembe helyezése, javítása, átalakítása vagy biztonsági tesztelése az üzemeltetésért felelős vezető által jóváhagyott terv alapján történhet*.

BIZALMAS vagy magasabb minősítés esetén, amennyiben a központi kiszolgáló helyiségekben több szervezet állományába tartozó személyek dogoznak, vagy nagy létszám szükséges a feladatok elvégzéséhez, *egyedi azonosítást lehetővé tévő megoldást kell alkalmazni* (név szerinti kitűző vagy fényképes belépési igazolvány, látogatói kitűző). Az állandó belépésre jogosultakról hiteles, naprakész listát kell vezetni, amelyet a helyiségben is el kell helyezni. A helyiségben dolgozó személyek számára feladatul kell meghatározni, hogy *ha egy személyt azonosító jelzés nélkül látnak, azonnal szólítsák fel az adott személyt az azonosításra, amelynek hiányában azonnal tegyenek jelentést a meghatározott szolgálati személy felé*. A kritikus fontosságú eszközöket a technikai védelmi rendszerbe bekötött hardver védelemmel kell ellátni, ami a burkolat megbontása, vagy az eszköz eltávolítás esetén azonnali riasztást generál.

Az elektromos hálózatot, az érintésvédelmet és a villámvédelmet a vonatkozó magyar szabványokban meghatározottak szerint kell kialakítani és fenntartani. Az energiaellátás biztonsága érdekében, ahol az szükséges:

- az egypontos meghibásodások veszélyeinek elkerülése érdekében többutas betáplálást kell alkalmazni, vagy
- tartalék áramforrást kell alkalmazni.

A tartalék áramforrás paramétereinek meghatározásakor figyelembe kell venni:

- az átkapcsolási időre vonatkozó követelményeket (automatikus vagy kézi indítás);
- a teljesítményre vonatkozó követelményeket úgy, hogy:
  - az elektronikus adatkezelő eszközök működése mellett képes legyen kiszolgálni az azok működéséhez szükséges segédüzemi (például klíma) berendezéseket, valamint biztosítsa a munkavégzéshez szükséges szolgáltatásokat (pl. vész világítás) is;
  - a tartalék kapacitás elegendő legyen a későbbi fejlesztések, bővítések kiszolgálására.

A tartalék áramellátás beindulásáig megfelelően méretezett, szünetmentes tápegységeket kell alkalmazni. Az erősáramú betáplálásokat, tartalék és szünetmentes áramellátást időszakosan ellenőrizni kell, beleértve a kezelő állomány gyakoroltatását is.

Amennyiben az üzemeltetett eszköz technikai leírása az életvédelmi földelés mellett biztonsági földelés kialakítását is igényli, a műszaki követelményeket egyedileg kell meghatározni. A biztonsági földelés használatba vétele csak a szükséges paramétereket igazoló mérési jegyzőkönyv alapján történhet. A biztonsági földelés megfelelőségét időszakosan ismétlődő ellenőrző mérésekkel kell igazolni, a mérésről szóló jegyzőkönyveket az üzemeltetett elektronikus adatkezelő rendszer biztonsági dokumentumai között kell tárolni.

Az üzemeltetett eszközök technikai paramétereinek figyelembe vételével szükség esetén antisztatikus kialakítást kell alkalmazni.

Az erős és gyengeáramú betáplálási pontokat, kábelvezetéseket elkülönítve kell kialakítani. A kábelek vezetésekor, kifejtésekor egyértelmű jelölési rendszert kell alkalmazni.

A helyiségek hőterhelésének tervezésekor figyelembe kell venni a várható bővítési igényeket is.

A fentiek szerinti eljárások, rendszabályok az üzemeltetők, felhasználók számára vélhetően nem ismeretlenek. *A tervezéshez szükséges idő és a kivitelezéshez szükséges anyagi erőforrások rendelkezésre állása esetén az általánosan körvonalazott környezet kockázatmentesen kialakítható*. A problémát az említett rendelkezésre állás jelenti. A pontos alkalmazói (hadműveleti) követelmények nélküli tervezés és az ezzel járó többszörös követelmény módosítás, az anyagi erőforrások tervezés közben történő módosítása, a beszerzések során bekövetkező változtatások mind olyan korlátok, amelyek a biztonságtudatos, lendületes követelménytámasztást még kezdeti szakaszban derékba törik.

A faburkolatú lépcsőfeljáró alatti, csak ráccsal elkülönített, évek óta üzemelő „ideiglenes” fájl és levelező szerver; a szellőztetési szükséglet miatt állandóan kitámasztott hátsó ajtó; javításban adott pótlás nélküli akkumulátor csoport; a biztonsági mentés ideiglenes hiánya vagy a mentőegység üzemképtelensége, a közművázlatokon nem szereplő – de is ismeretlenül fenyegető viszonylatok –, illetve az öltöző-, iroda-, raktár-, műhely-, szerverterem követelményei szerint üzemeltetett multifunkcionális helyiségek elrettentő, a rendezettséget célzó állapot ellen ható példák lehetnek.

Gyakran félreéréseket okoz a biztonsági követelmények között olvasható „megfelelő szintű”, „szükség szerinti” vagy a „helyi sajátosságoknak megfelelő” kifejezés. A bevezetésben megfogalmazottak szerint könnyen belátható, hogy minden rendszerre, *minden környezetben és minden sajátosságnak megfelelő rendszabály halmaz nem állítható elő*. Ezért van szükség a hierarchizált szabályozásra, és annak megértésére, hogy *egy helyszín rendszer esetében nem lehet a keret jellegű központi követelményt megismételni, hanem pontos paramétereket kell meghatározni, melyet elemzéssel, tesztekkel kell megalapozni*.

Érdemes megjegyezni *az üzemeltetési környezet perspektivikus menedzselésének feladatát is*. A gazdasági nehézségek miatt gyakoriak a minimál szintet biztosító vagy

csökkentett szolgáltatást nyújtó beruházások (a tervekben az „erőforrások függvényében később kerül biztosításra” címmel szereplő fejezet), amelyek miatt *hullámokban történik meg a szükséges képességek kialakítása*. A minimális eszközben való gondolkodás gyakran eltakarja az üzemeltetési környezet feszítő problémáit (áramellátási vagy légkondicionálási technikai korlát, méret vagy tetőterhelés miatti gondok), illetve az egymásra kifejtett hatásokat, és korlátozhatják a meghatározott képességek kialakítását, rendelkezésre állását.

3. A KARBANTARTÁSRA VONATKOZÓ KÖVETELMÉNYEK

Az adatkezelő eszközöket a gyártó (szállító) által ajánlott szervizelési időközönként és előírások szerint kell karbantartani. A tervezett karbantartásokról az üzemeltetési kör szerint kialakított karbantartási tervet kell készíteni. A karbantartási tervek kialakításakor gondoskodni kell arról, hogy:

- minden karbantartást igénylő eszköz *valamelyik karbantartási tervben szerepeljen*;
- *a tervek között átfedés ne legyen* illetve a műszakilag egy karbantartási körbe tartozó, de eltérő üzemeltetési rend miatt *más karbantartási tervbe tartozó elemek karbantartása összehangoltan történjen*;
- a végrehajtott karbantartások ellenőrzésével és nyilvántartásával biztosított legyen a tervek végrehajtásának naprakész figyelemmel kísérése.

Karbantartást, javítást csak a szükséges technikai ismeretekkel rendelkező, feljogosított személy végezhet. A rendszer-specifikus üzemeltetési dokumentumokban *azonosítani kell azokat az eszközöket, elemeket, amelyek karbantartása speciális felkészültséget igényel*.

A gyanított vagy tényleges hibáról, valamint megelőző és javító karbantartásról feljegyzést kell készíteni, amelyet a rendszer-specifikus üzemeltetési dokumentumokban rögzített követelmények szerint kell megőrizni.

A tervezett karbantartásokról *a felhasználókat a rendszer-specifikus üzemeltetési dokumentumokban meghatározott módon előzetesen tájékoztatni kell*. A tájékoztatásban meg kell határozni azt az eljárást, amely segítségével a felhasználó közölheti a tervezett folyamat idejével kapcsolatos akadályközlését vagy kiegészítő információt kérhet.

Amennyiben a karbantartás a felhasználói feladatok szervezeti kockázatokkal járó kiesését okozzák, a karbantartás idejére tartalék adatkezelési szolgáltatást kell biztosítani. *A tartalék adatkezelési szolgáltatásnak csökkentett képességek esetében is biztosítania kell a biztonsági osztály szerinti védelmi rendszabályokat*.

Minősített elektronikus adatkezelő eszköz szervezeten kívüli karbantartása vagy javítása a szükséges telephely biztonsági tanúsítvány megléte esetén engedélyezhető, az adathordozó eltávolítása mellett. Beépített adathordozó esetén a művelet elvégzéséhez kiegészítő védelmi rendszabályokra van szükség.

Alap vagy fokozott biztonsági osztályba tartozó adathordozók esetén a szükséges törlési eljárást, vagy adathordozó eltávolítást és az ezekkel kapcsolatos ellenőrzési feladatokat a rendszer-specifikus biztonsági dokumentumokban kel meghatározni. Magasabb biztonsági osztályú adat esetén ezek a megoldások csak *az illetékes hatóság által jóváhagyott eljárások lehetnek*.

A rendszer-specifikus üzemeltetési és biztonsági dokumentumokban meg kell határozni *a szervezeten kívüli karbantartás végrehajtásához szükséges előkészületi, végrehajtási és utólagos ellenőrzési feladatokat*. Érzékeny adatok esetében az adathordozók megsemmisítése vagy javításban küldése közötti döntés meghozatalát kockázatelemzéssel kell megalapozni.

Elektronikus adatkezelő eszköz rendszerből történő végleges eltávolítása vagy javítás, karbantartás céljából történő ideiglenes eltávolítása a rendszer-specifikus üzemeltetési dokumentumban meghatározott vezető engedélyezésével, a biztonságért felelős személy

hozzájárulása esetén történhet. Az engedélyeztetésre vonatkozó eljárásrendet részletesen ki kell dolgozni, és a szabályokat az üzemeltető állománnyal ismertetni kell.

Az eltávolított eszköz azonosításához szükséges adatokat az üzemeltetés helyszínén, valamint a szállítólevélen, átadás-átvételi jegyzőkönyvben pontosan fel kell tüntetni.

A külső javítás, karbantartás végrehajtása után az eszköz *rendszerbe történő illesztése előtt ellenőrizni kell az eszköz azonosságát, teljességét és funkcionális működését*. Az eszköz ellenőrzés után, a biztonságért felelős személy jóváhagyása esetén illeszthető vissza a rendszerbe. Amennyiben az eszközön olyan mértékű változtatások történtek, melynek eredményeképpen egyértelműen nem határozható meg a rendszerbe történő illesztés biztonsági hatásai, *biztonsági tesztet kell végrehajtani*.

Az üzemeltetési időszakra vonatkozó fenntartási támogatás hiányossága vagy hiánya *hatékony támadás lehet az információ biztonságpolitikában meghatározott biztonsági cél (a rendelkezésre állás, sértetlenség vagy bizalmasság) ellen*. Az egyszerűen megfogalmazott rendszabályokon keresztül is jól látható, hogy a karbantartási vagy javítási tevékenységet komplexen kell megközelíteni. A fentiekben *biztonság szempontjából megfogalmazott feladatok nagy biztonsággal azonosíthatók az üzemeltetésre vonatkozó ajánlásokkal vagy nemzetközi szabványokkal*. Emiatt a gyakorlatban nincs szükség arra a kérdésre, hogy „mit és miben szabályozzunk”. A biztonsági szabályozásnak követelményeket kell meghatározni, az üzemeltetési szabályoknak pedig részletes, követhető ellenőrizhető eljárásrendben meg kell határozni az alkalmazandó technikai vagy szervezési lépéseket.

4. A FELÜGYELET NÉLKÜLI RENDSZERELEMEK FIZIKAI BIZTONSÁGA

A felügyelet nélküli rendszerelemek elhelyezésére szolgáló helyiségeket olyan behatolás érzékelő és jelző rendszerrel kell ellátni, amelyek a meghatározott riasztási paramétereket képesek a reagáló erőkhöz továbbítani.

Az épületek, helyiségek fizikai kialakítását, ellenálló képességét a reagáló erők kiérkezési idejéhez kell méretezni. Az érzékelő és riasztó rendszereket valamint a reagáló erők tevékenységét időszakosan ellenőrizni kell. A reagáló erőknél szolgálatba álló új alkalmazottal a helyszínen kell megismertetni a szükséges védelmi feladatokat.

Az elektronikus adatkezelő rendszer azon elemeit, amelyek az MH szempontjából fokozottan védendő üzemeltetési adatokat tartalmaznak, a fizikai védelem megerősítése érdekében adattörlést, kulcsmegsemmisítést, kritikus elem önmegsemmisítését végző mechanizmusokat, illetve a felügyeleti központba történő automatikus jelentés mechanizmust kell kialakítani. *A szükséges védelmi rendszabályokat kockázatelemzéssel és értékeléssel kell megalapozni*.

5. A RENDEZVÉNYEK BIZTOSÍTÁSÁRA VONATKOZÓ FONTOSABB KÖVETELMÉNYEK

Minősített adatot elektronikusan feldolgozó rendezvény esetén a rendezvény biztosítási tervet ki kell egészíteni az elektronikus biztonságra vonatkozó intézkedésekkel, hálózat esetén el kell készíteni a rendszer-specifikus biztonsági dokumentumokat (vagy a meglévőt ki kell egészíteni), és *szükség esetén a védelmi rendszabályok megfelelőségét az illetékes hatósággal akkreditáltatni kell*.

A rendezvény helyszínén *azonosítani kell a nyilvánosan látogatható területeket, adminisztratív zónákat és biztonsági területeket*. A rendezvény előkészítésének befejezésekor ellenőrizni kell a rendezvény területét. A résztvevők számára szükség esetén biztosítani kell az adathordozók, hordozható eszközök megbízható őrzését:

- átviteli elismervény alapján;
- személyi azonosítás esetén;

- az átvett anyagok jelölésével.

A rendezvényen a tartalék, vagy használaton kívüli eszközöket elkülönítve, nyilvántartva és a hozzáférést szabályozva kell tárolni. A rendezvény szüneteiben az elektronikus adatkezelő eszközök és adatok biztonsága érdekében:

- a nem használt helyiségeket zárva vagy felügyelet alatt kell tartani, vagy
- az eszközöket, adathordozókat erre a célra kijelölt helyiségben kell őrizni.

A rendezvényen rendszabályokat kell foganatosítani *a felügyelet nélkül hagyott eszközök, adathordozók ellenőrzésére és begyűjtésére. A biztonsági területek belépési pontjainál lehetőséget kell biztosítani a mobil telefonok őrzött ideiglenes tárolására*.

Ideiglenes kialakítás esetén is biztosítani kell az elektromos kábelek vonalvezetésére, rádiófrekvenciás szűrők alkalmazására, a rendszer környezetében alkalmazható berendezésekre, elektromágneses árnyékolástechnikai megoldásokra, illetve csökkentett kisugárzású hardver eszközök alkalmazására, valamint a rendszerhez tartozó fém berendezések földelésére vonatkozó előírások érvényesülését.

Naprakész nyilvántartást kell vezetni az alkalmazott hardver és szoftver elemekről, kisegítő eszközökről, illetve a rendezvény után ezen eszközök esetében is a szükséges törlési vagy megsemmisítési eljárásokkal kell megakadályozni az illetéktelen megismerést.

Az adathordozók biztonságát (beleértve az esetleges szállítási feladatokat is) a dokumentumbiztonsági követelményeknek megfelelően kell biztosítani.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A cikk a fizikai védelem és az üzemeltetési környezet általánosan megfogalmazható, fontosabb kérdéseinek összefoglalásával biztonsági szempontokra koncentrál, láthatóvá téve az átfogó megközelítés, az életciklus szemlélet szükségességét ezeken a területeken is.

A rendszabályok, illetve az említett példák mutatják a bizalmasság, sértetlenség és rendelkezésre állás veszélyeztetésének lehetőségeit. Jól látható, hogy az adatok, adatkezelő képességek nem csak a felhasználókon, felhasználói eszközökön keresztül, hanem az infrastruktúrán keresztül is fenyegethetők eszközökön, támogató szolgáltatásokon, eljárási hiányosságokon vagy személyeken keresztül. Ez a szempont a kormányzati szinten megindult kritikus infrastruktúra védelmi (KIV) feladat fontosságát igazolja. Az elektronikus adatkezelés védelme területén a kritikus információs infrastruktúra védelmi (KIIV) feladat a kijelölés, védelmi igény azonosítás és fenntartás részei az IT tervező, üzemeltető, és a információbiztonsági állomány szoros együttműködését igényli, a szükséges mértékű rendelkezésre állás biztosítása érdekében.

Az üzemeltetés fentiekben vázolt kérdései nem képzelhetők el hatékony kockázatelemzés és menedzselés-, biztonsági teszt-, konfiguráció menedzselés-, illetve a folytonossági tervezés (BCP) és a helyreállítás (DRP) rendszer-specifikusan kidolgozott feladatai nélkül, ami óhatatlanul is mutatja, hogy jelentős feladatok állnak az üzemeltetési és biztonsági kérdések tanulmányozói előtt.

HIVATKOZÁSOK

[1] 90/2010. (III. 26.) Korm. Rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[2] MSZ ISO/IEC 27001:2006, Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények

[3] 27002 MSZ ISO/IEC 17799:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (MSZ ISO/IEC 27002)

[4] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1. 1. 2008

[5] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról

Jéri Tamás – Pándi Erik – Jobbágy Szabolcs
jeri.tamas@gmail.com – pandi.erik@zmne.hu – jobbagy.szabolcs@zmne.hu

A HÁLÓZATOK VÉDELMI ASPEKTUSAI[1]

Absztrakt

Jelen közlemény az IT hálózatok védelmének kérdéseit világítja meg.

This publication sheds light on questions related to the defence and security of IT networks.

Kulcsszavak: *IT hálózat, védelem ~ IT network, protection*

BEVEZETÉS

A témakört tekintve legfőbb cél a biztonság elérése. Az informatikai biztonság, az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[2] Az informatikai biztonság sajnos nem egy alapértelmezett állapot, eléréséhez aktívan tevékenykedni kell, védelmet kell kiépíteni.

1. A VÉDEKEZÉSI TEVÉKENYSÉG

A védekezés az a cselekvés, amikor megvédünk valakit vagy valamit a támadástól; védelem, megvédés.[3] A védés megakadályozza azt, hogy megtámadjanak valakit vagy valamit, illetve, hogy elfoglalják.[4] A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk. 22 Az informatikai védelem a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának védelme.”

2. VÉDENDŐ HÁLÓZATOK

A hálózatok minden fajtáját egyaránt védeni kell, azonban a rendszerek jellegéből adódóan eltérőek a hangsúlyos pontok, a megvalósítás gyakorlata, illetve módszere.

- Internetbe kötött szerverek

Speciális védendő „hálózatnak” tekinthetők, még akkor is, ha csak egyetlen szerverről van szó. Távoli hozzáférés révén úgy kell megoldani a védelmet, hogy egyrészt biztosítva legyen a szerver teljes körű adminisztrációs lehetősége, másrészt minimális legyen a támadhatóság.

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült
2 Dr. Muha Lajos : Informatikai Rendszerek Biztonsága – Előadás 2009.
3 http://wikiszotar.hu/wiki/magyar_ertelmezo_szotar/Védekezés
4 http://wikiszotar.hu/wiki/magyar_ertelmezo_szotar/Véd

- Belső hálózatok
    a) Zárt hálózatok

Ezen hálózatok valószínűleg annyira érzékeny adatokat tartalmaznak, melyek követelményként támasztják a zárt jelleg fenntartását. A védelmet az adatok ki,- és bekerülésének, illetve a hálózat szándékos kinyitásának megakadályozására kell összpontosítani.

b) Félig nyitott hálózatok

A legösszetettebb védelmet igénylő hálózati jelleg, mert a zárt hálózatoknál és az Interneten működő szervereknél kialakított megoldásokat ötvözve kell alkalmazni. Figyelni kell az Internet felöl érkező támadások kivédésére, és a lehető legjobban kell érvényesíteni a zárt jelleget annak ellenére, hogy a hálózatból létezik kilépési pont.

3. SZOLGÁLTATÁS VS. VÉDEKEZÉS

Előfordul, hogy ismerőseink megkérdeznek: vajon lehet-e feltörhetetlen szervert telepíteni? Melyre válaszunk, hogy azt a világ legegyszerűbb dolga létrehozni, melyet persze kétkedve fogadnak. Példaként az ajtó nélküli ház esetét szoktuk említeni: vajon be lehet-e törni egy olyan házba, melynek csak falai, és teteje van? A válasz egyértelműen nem, mely szimbolikusan hasonlít a szolgáltatás nélkül működő szerver esetére. Bármely szerver tehát hálózaton keresztül támadhatatlan, amennyiben nem működik rajta szolgáltatás, melyen keresztül adatcserét lehetne végrehajtani. A problémát pontosan az jelenti, hogy szervereket a szolgáltatások működtetése miatt üzemeltetünk. Tehát bármely szolgáltatás elindítása egyrészt egy alapfeladat működtetését, másrészt egy biztonsági kockázat megjelenését indukálja. Több szolgáltatással működő szerver természetesen nagyobb kockázatot jelent, főleg, ha azok közül valamelyik az operációs rendszer karbantartását szolgálja. Az Internetes kiszolgálók gyakran nagy távolságra üzemelnek annak tulajdonosától, ezért megkerülhetetlen a távoli elérés biztosításának és a megfelelő védelem kiépítésének problematikája.

4. A VÉDEKEZÉS ESZKÖZEI

Tűzfalak építése

A tűzfal (angolul firewall) célja a számítástechnikában annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás.[5] Tűzfalat minden IP címmel rendelkező hálózati eszközre lehet telepíteni, ugyanakkor kiemelt jelentősége a belső hálózatok ki,- belépési pontján, valamint az Internetes kiszolgáló szervereken van. A tűzfalmegoldásokra általános érvényű szabály, hogy alapértelmezésben minden tilos, kivéve, amit szabad.

- Packet filter firewall – csomagszűrő tűzfal

Egy statikus szabálygyűjtemény alapján továbbítja, vagy eldobja a csomagokat. A szűrési feltételek protokoll fejlécekre vonatkoznak, a csomag tartalmára nem, ezért gyors tűzfal típus. A fejlett csomagszűrők csendben, visszajelzés nélkül, az elavultabbak visszajelzéssel dobják el a csomagokat. A csomagszűrés a tűzfalak leggyakrabban használt fajtája, ma már a legolcsóbb routerekben is rendelkezésre álló lehetőség.

- Circuit-level firewall – kapcsolat alapú tűzfal

Előre definiált szabályok alapján működik, viszont nem csomagokat, hanem kapcsolatokat kezel. A kapcsolatépítést figyeli, rövid ideig figyelemmel kíséri, majd dönt

5 http://hu.wikipedia.org/wiki/Tűzfal_(számítástechnika)

annak biztonságosságáról. Pozitív elbírálás után tovább már nem vizsgálódik, a kapcsolathoz tartozó csomagokat átengedi. Mivel csomagokat nem, csak kapcsolatokat vizsgál, ezért gyorsabb lehet a csomagszűrő tűzfalnál is.

- Application gateway firewall – alkalmazás szintű tűzfal

A hálózatok közötti minden kommunikációt szétvág, és közvetítőként biztosítja a kapcsolatot. Az OSI[6] modell minden szintjén ellenőriz, és teljes vizsgálatot végez, ezért meglehetősen lassú, továbbá speciális szolgáltatás működését ismeret hiányában nem képes ellenőrizni.

Rosszindulatú programok távoltartása

A vírusok, kémprogramok és általában a rosszindulatú programkódok távoltartására kitalált védekező eszköz, mely a háttérben folyamatosan futó alkalmazásként van jelen. A munkaállomások és a szerverek védelmére egyaránt használatos, ugyanakkor fontos megjegyezni, hogy elsősorban az elterjedt, megengedő típusú operációs rendszereken terjednek a rosszindulatú programok, ezért alkalmazásuk főleg ott jellemző. Az alkalmazott távoltartó programok – általában - saját adatbázissal rendelkeznek, melyben a rosszindulatú kódok vannak nyilvántartva, ezért folyamatosan szükséges az adatbázisok frissítése, a legújabb kártékony programok elleni sikeres védekezés érdekében.

A védekező szoftvereknek vannak kedvezőtlen hatásai is, mert az állandó jelenlét elvonhatja az erőforrásokat, mely főleg a kisebb kapacitású számítógépeknél vehető észre, továbbá a frissítési adatbázisok több megabájtos mérete jelentős hálózati forgalmat generálhat.

Titkosítás

A titkosítás alkalmazása nagyon hosszú időre nyúlik vissza, azonban célkitűzése mindvégig az volt, hogy a küldő által küldendő eredeti – nyílt – szöveget oly módon tegye értelmezhetetlenné, hogy harmadik személy birtokában ne legyen információértéke, azonban a címzett képes legyen a kódolt szövegből, az eredeti előállítására.

Ez a lehetőség a számítógép-hálózatokban alkalmazott kommunikációban is kiaknázható, melyet a küldendő – érzékeny – adatok nagy mennyisége is alátámaszt. A titkosítás alkalmazása a szolgáltatások nagy részében rendelkezésre, így biztonságosan lehet:

- leveleket, állományokat küldeni és fogadni;
- távoli adminisztrációt végezni;
- hálózatokat összekapcsolni;
- böngészni az Interneten, stb.

Komoly matematikai kutatások eredményeként többféle titkosítási eljárást fejlesztettek ki, azonban mindegyikre igaz, hogy, egy kulcs segítségével hozza létre a titkos szöveget (ciphertext-et). A szimmetrikus kulcsú titkosítás problémája, hogy a kulcsban az adónak és a vevőnek meg kell egyeznie, azt egymásnak át kell adni, melyre rendszerint ugyanaz a kommunikációs csatorna áll rendelkezésre, s a kulcs megszerzésével a rosszindulatú támadó vissza tudja fejteni, a titkosított szöveget is. A problémára megoldást jelentett a nyilvános, aszimmetrikus kulcsú titkosítás.

A(z) N(T(x))=x és T(N(x))=x képletben ’T’ a titkos, ’N’ a nyilvános kulcsot, ’x’ pedig a kódolandó információt szimbolizálja. A két kulcs együttes alkalmazása szükséges a

6 Open Systems Interconnection Reference Model, magyarul a Nyílt rendszerek Összekapcsolása

titkosított információ visszanyeréséhez, így a széles körben ismertetett 'N' kulcs, a titkosító - kizárólagos - birtokában levő 'T' kulcs nélkül nem alkalmas a dekódolásra.

Az aszimmetrikus titkosító kulcs előnye a biztonságos kulcscsere, hátránya a lassúság, a szimmetrikus kulcs előnye a gyorsaság, hátránya a biztonságos kulcsátadás problematikája. A mai korszerű (SSL[7]) titkosítási eljárásoknál a vegyes használat a jellemző, amikor a kapcsolatépítés aszimmetrikus, majd a tényleges adatcsere szimmetrikus titkosítási kulccsal hajtódik végre.

Proxy használata

„Számítógép-hálózatokban proxynak, helyesebben proxy szervernek (angol „helyettes", „megbízott", „közvetítő") nevezzük az olyan szervert (számítógép vagy szerveralkalmazás), ami a kliensek kéréseit köztes elemként más szerverekhez továbbítja."[8] Mivel a proxy közbenső elem a tényleges kliens és szerver között, beavatkozásra ad lehetőséget, feltételhez kötheti, hogy mit továbbít a kliens felé. A proxy szerver lehetséges használata:

- átmeneti tárolóként (cache) megvalósított gyorsítás;
- tűzfal funkciók alkalmazása;
- kapcsolatok szűrése.

A proxy megoldások több szolgáltatási funkcióra is rendelkezésre állnak, de a legelterjedtebb a web-proxy, mellyel egy belső hálózatból biztosítható, hogy a felhasználók

- közvetlen web kéréseket ne tudjanak az Internet felé indítani;
- a gyakrabban látogatott oldalak tartalmát gyorsabban megkapják;
- csak a munkájukhoz szükséges oldalakat látogathassák;
- nem kívánt adattartalmat ne tudjanak a munkaállomásukra letölteni.

ezáltal ne tudják kitenni a belső hálózatot támadásnak.

Egyéni – ismeretlen – megoldások alkalmazása

Hasonlóan a hétköznapi élethez, a számítógép-hálózatba betörő sem számíthat minden körülményre. A váratlan „fogadtatás", az egyéni kreatív védelmi intézkedések nagyban megnehezíthetik a támadók dolgát, sőt jó eséllyel meg is gátolhatják a behatolást. A védelem feladatai között szereplő észlelés és reagálás együttesen alkalmazható, ha felkészülünk egyes események bekövetkezésére, és kidolgozott tervünk van a reakció végrehajtására.

Az egyéni megoldások kialakítására általában operációs rendszer szinten van lehetőség, mely jól kamatoztatható tűzfalak, átjárók, vagy saját internetes szerver üzemeltetése esetén. Itt meg is jegyezném, hogy egyéni védelmi intézkedést nem lehet, vagy nagyon nehéz alkalmazni célhardvereken. Gyakran halljuk, hogy a legbiztonságosabb tűzfalak hardveresek, aminek biztosan van igazságtartalma, de hogy az operációs rendszereken megvalósított tűzfalakhoz képest kicsi a reagálási képesség, abban biztos vagyok. A hardverekben általában bedrótozott mechanizmusok állnak rendelkezésre, melyek kevés mozgásteret adnak.

7 Secure Socket Layer – biztonsági alréteg, mely a szállítási és valamely alkalmazási réteg között helyezkedik el

8 http://hu.wikipedia.org/wiki/Proxy

5. ÁLTALÁNOS VÉDEKEZÉSI MECHANIZMUSOK

Minden általánosságban alkalmazható védelmi intézkedést meg kell tenni, a lustaság nem kifizetődő. Ebben a részben megpróbáljuk összefoglalni azokat a kötelezően alkalmazandó védelmi intézkedéseket, melyek az alacsony befektetéshez képest, nagyban növelik a rendszerek védelmét.

Általános védelmi intézkedések:

- Operációs rendszerek, alkalmazások frissítése

A programok gyártóinak konkurencia harca gyakran hibás, vagy biztonsági réseket tartalmazó kódok fejlesztéséhez vezet. A nyilvánosságra kerülő hibák kihasználhatók, gyenge láncszemek, ezért a gyártók által kiadott javításokat szükségszerű alkalmazni. A programok készítői – általában – internetes frissítő oldalak üzemeltetésével biztosítják a legfrissebb javítócsomagok letöltését.

- Rosszindulatú programok adatbázisainak frissítése

Hiába működnek rosszindulatú kódokat távoltartó programok, ha azoknak adatbázisai nem naprakészek és nem ismerik fel a legújabb kártékony programokat. A folyamatos frissítés tehát elengedhetetlen a biztonság szinten tartásához.

- Internet elérés szabályozása proxy szerver alkalmazásával

Használata a fentebb leírt előnyök miatt javasolt, növeli a biztonságot. Alkalmazásának kétféle megközelítése jellemző. A megengedőbb, a nemkívánatos weboldalak felsorolásával, a tiltóbb az engedélyezett oldalak deklarálásával biztosítja a működést.

- Jogosultságok alkalmazása, jelszavak kikényszerítése

A felhasználók megszemélyesítése account-ok alkalmazásával valósítható meg. Ahol lehetőség van rá, használni is kell, hisz elhagyásával a támadók dolga nagyban megkönnyíthető. Hasonlóan fontos a megfelelő bonyolultságú jelszavak kikényszerítése, illetve az alapértelmezett jelszavak megváltoztatása, mellyel nagyban megnehezíthető a támadási tevékenység. A felhasználói hozzáférések kialakításával, jogosultsági szintek beállítására nyílik lehetőség, mellyel meghatározható a rendszerben tárolt adatok (állományok, adatbázisok) illetékessége.

- Titkosított csatornák alkalmazása

Használatával megakadályozható, megnehezíthető az egyszerű lehallgatással, szaglászással történő információszerzés. Kiváló – ingyenes – titkosító eljárások állnak rendelkezésre, melyek alkalmazása bonyolítja a szolgáltatások konfigurációját, ugyanakkor nagyban növeli a biztonságot.

- Hálózati eszközök elzárása

A rendszerben működő hálózati elemek fizikai hozzáférésének megakadályozására zárható helyiségeket, szekrényeket kell használni, melyek képesek az illetéktelen személyeket a rendszertől távol tartani.

- Használaton kívüli végpontok inaktiválása

A támadók szeretnének csatlakozni a hálózathoz, ezért keresik az elhagyatott aktív hálózati végpontokat. A nyilvántartásokat folyamatosan aktualizálni kell, s a magára hagyott végpontokat pedig kötelező inaktiválni.

- Felhasználói fluktuációk követése

A munkáltatóknál bekövetkező fluktuációt kötelező az információ-technológia szintjén is követni, mellyel szavatolható, hogy - mindig - csak és kizárólag az aktív dolgozóknak legyen hozzáférésük a rendszerhez. A bosszúsan távozó munkatársak - aktívan hagyott belépési kódjukkal – kellemetlenséget okozhatnak.

- Hálózati információk elrejtése

Minden hálózatban léteznek olyan – a működést meghatározó – beállítások, adatok, melyeket eltitkolni ugyan nem lehet, de kerülendő velük hivalkodni. Egyrészt célszerű az IP címeket névfeloldással helyettesíteni, másrészt feltűnés nélkül használni a tűzfal,- átjáró,- proxy,- adatbázis-szerverek címeit.

- Szolgáltatások biztonságos beállítása

Manapság a szolgáltatások konfigurációs lehetőségei annyira sokrétűek, hogy az üzemeltetőnek gyakran döntenie kell az egyszerűbb használat,- nagyobb kockázat, vagy a bonyolultabb beállítás,- nagyobb biztonság mellett. Véleményünk szerint vállalni kell a nehézkesebb konfigurálást, de mindenképpen törekedni kell a biztonságos üzemeltetésre (pld. FTP szerver gyökér könyvtár meghatározása).

- Használaton kívüli szolgáltatások kikapcsolása

Ma egy operációs rendszer telepítése után, szerver és munkaállomás tekintetében egyaránt rengeteg használaton kívüli szolgáltatás működhet. Mivel minden hálózati szolgáltatás üzemeltetése biztonsági kockázat, a feleslegeseket ki kell kapcsolni, ezáltal erőforrás takarítható meg és csökkenthető a támadási felület.

- Adatbázis hozzáférések korlátozása

A féltve őrzött adatokhoz történő hozzáférés - szakszerű - beállítása alapkövetelmény. A hálózati porton figyelő adatbázis-kezelők (pld. Oracle, MySql) a megfelelő kliens programokkal megszólíthatók, csatlakozási kérések indíthatók. Alkalmazásuk esetén, amíg lehetséges kerülni kell a nyilvános hozzáférés beállítását, ha viszont elengedhetetlen, akkor jelszavakkal és lehetőleg titkosított csatornán keresztül kell az elérhetőséget biztosítani. Az adatbázis-kezelőkkel kapcsolatban az elérhetőség mellett létfontosságú a hozzáférési szintek alkalmazása, az elégséges jogosultságtól többet kiadni tilos. (Például lekérdezési tevékenységhez felesleges módosítási jogot adni az adatbázis-kezelőben.).

- Tűzfalak használata

A szolgáltatások túlterhelése (DOS, DDOS) elleni védelem, továbbá a hálózati kapcsolatok megfelelő mederben tartásának alapvető eszköze a tűzfal. Alkalmazása nélkül mind a hálózatok, mind a szerverek veszélynek vannak kitéve, ráadásul – lelkes fejlesztők százainak köszönhetően - alacsony költségvetéssel is kiváló tűzfalak építhetők.

- Mentések végrehajtása

Hálózatok üzemeltetésekor kötelező rendszeresen mentéseket végezni, melyekből nem várt események bekövetkezése esetén, visszaállíthatók az elveszett adatok. Az automatizált, rotációs rendszerű archiválások a legcélszerűbbek, a rendszeres visszaellenőrzések végrehajtása mellett. Az archívumokat célszerű a szerverszobától elkülönítetten, jól elzárható helyen tárolni.

- Rendszerállományok jogosultságainak ellenőrzése

A - szerverek operációs rendszerein fellelhető - rendszerállományok jogosultsági beállításai, megfelelő védelmet biztosítanak a véletlen, vagy szándékos károkozás, továbbá

az adminisztrátori jogok megszerzése ellen. A kielégítő állapot ellenőrzésére szkriptek, programok állnak rendelkezésre, melyek futtatásával meg lehet győződni az operációs rendszer sértetlenségéről.

- Jelszavak biztonságos tárolása

Az operációs rendszerek jelszavainak kezelése és tárolása biztonságosabb, ha azok, a felhasználói nevektől külön helyen, úgynevezett - különleges jogosultsági szinttel rendelkező - árnyék állományokban kerülnek elhelyezésre.

A mai modern kiszolgáló programokban lehetséges az adatbázis alapú azonosítás, amikor a felhasználók hozzáférési adatai táblákban és rekordokban helyezkednek el. Ezzel a megoldással operációs rendszer szinten nem keletkeznek hozzáférések, így a szolgáltatások lehallgatásával nem szerezhető közvetlen hozzáférés.

- Levelező szerver rendszerbeállítása

A hálózatok védelmében, kulcsfontosságú szerepe van az elektronikus levelek kezelésének. Az internet szolgáltató által biztosított SMTP[9] szerver és a munkaállomások levelező kliensei közé célszerű saját – vírusfigyelő és kéretlen levél ellenőrző funkcióval felruházott – levelezőszervert iktatni, mely hatékony védelmet biztosít, a levélben érkező kártevők ellen. A levelezőszerver tovább finomítható Webmail[10] alkalmazásával, mely rugalmassá teszi a levelek figyelését, csökkenti a hálózati adatforgalmat, és mellőzi a munkaállomások levelező klienseinek használatát.

Felhasználóknál, munkaállomásokon alkalmazandó védelmi intézkedések:

- Felhasználók oktatása

A felmérések szerint 90 %-ban a felhasználók jelentik a biztonsági kockázatot, ezért kötelező őket rendszeres oktatásban részesíteni. Tudniuk kell, hogy a jelszavakat miért kell bizalmasan kezelni, mit jelent a social engineering és mit jelent a hálózatok védelme.

- Szkript nyelvek tiltása

A munkaállomások támadása gyakran többletfunkciókat biztosító szkript nyelvek használatával valósul meg, melyek alkalmazása opcionális. A megfelelő arányú tiltások és engedélyezések beállításával, elviselhető mértékűre csökkenthető a kockázat.

- Munkaállomások lockolása

Tipikus felhasználói magatartás a használatban levő munkaállomás felügyelet nélkül hagyása, gyakran alkalmazói programok futtatása közben is. Ezeknek az eseteknek elkerülésére mindenképpen fel kell hívni a felhasználók figyelmét, továbbá bizonyos üresjárati idő eltelte után szerver oldalon kezdeményezni kell a kapcsolat megszakítást, vagy kliens oldalon a jelszavas képernyő-kímélő indítását.

- Interfészek tiltása

A felhasználók előszeretettel szeretnék munkahelyükre bevinni, s ott használni saját adathordozóikat (CD/DVD/pendrive), melyek akár kártékony programokat is tartalmazhatnak. A munkaállomások felesleges interfészeinek tiltásával, a veszélyes alkalmazások, programok bejutását, illetve érzékeny adatok kijutását lehet megakadályozni.

9 Simple Mail Transfer Protocol
10 Web alapú levelező program

- Indítási jelszavak alkalmazása

Amennyiben köztudott, hogy a hálózat munkaállomásaihoz – például takarítási céllal – külső személyek fizikailag hozzáférnek, érdemes BIOS felhasználói jelszót használni, mely képes megakadályozni a munkaállomás indítását.

- Korlátozott jogok alkalmazása a munkaállomásokon

Beállításával egyrészt megakadályozható, hogy a felhasználó programokat telepítsen, töröljön, vagy módosítson a munkaállomáson, másrészt szavatolható, hogy az alkalmazott hálózati, biztonsági és egyéb beállítások ne változzanak meg.

6. ELKÉPZELÉSEINK

Az előző alfejezetben kitértünk az egyéni megoldások alkalmazására, melyek a váratlanság, vagy az ismeretlenség erejével erősítik a hálózatok védelmét. A bemutatásra kerülő megoldások kifejlesztését a hétköznapi élet tette szükségessé.

Szolgáltatások leállítása, indítása

A távoli szervereken egyszerre megvalósítandó biztonságos üzemeltetés és a teljes körű adminisztrációs tevékenységek között ellentmondás húzódik. Több távoli webszervert is üzemeltetünk Debian GNU Linux operációs rendszerrel, alfanumerikus környezetben. A szervereken a HTTP(S), SMTP, FTP kiszolgálók végzik a szolgáltatási feladatokat, azonban az adminisztrációs tevékenységek miatt titkosított shell-t, azaz SSH kiszolgálót is működtetni kell.

Az SSH az operációs rendszer vezérlésének kulcsa, mert közvetlen bejelentkezési lehetőséget, azaz adminisztrációs tevékenységet biztosít. Aszimmetrikus kulcsú titkosítást használ, tehát kicsi az esélye, hogy lehallgatással megszerezzék a bejelentkezési azonosítót vagy jelszót, ugyanakkor „biztosítja” a próbálgatást, azaz a véletlen bejelentkezés lehetőségét, továbbá erőforrásokat von el.

A problémát tehát két ellentétes érdek okozzák:

- az operációs rendszer és a szolgáltatások normális működése esetén az SSH egy „kolonc”, mert biztonsági kockázatot jelent és viszi az erőforrásokat;
- bármilyen szolgáltatási, vagy operációs rendszer szintű probléma esetén az SSH az egyetlen megoldás a beavatkozásra, hiányában utazni kell a szerverhez.

Ennek az ellentétnek a feloldására kerestük a kielégítő megoldást, és arra a következtetésre jutottunk, hogy amennyiben az SSH-t valahogy ki-be lehetne kapcsolgatni, akkor „a kecske is jóllakna és a káposzta is megmaradna”, hisz leállítása esetén megszűnne a kapcsolódás lehetősége, és vele együtt a biztonsági kockázat, bekapcsolása esetén pedig ismét rendelkezésre állna, tehát végrehajtható lenne minden adminisztráció.

Egyértelművé vált, hogy a feladat csak az „állandó” szolgáltatásokon keresztül valósítható meg, amennyiben képesek az SSH indítására, vagy leállítására, ami azonban rendszeradminisztrátori (root) jogosultságokba ütközik, amivel egyetlen „állandó” szolgáltatás sem rendelkezik.

A tervünk egy böngészővel meghívható, webszerver által futtatandó program létrehozása volt, mely URL[11] paramétereken keresztül vizsgálja a jogosultságot és dönt az SSH indításáról, vagy leállításáról. Az adminisztrátori jogok szükségessége miatt a feladatot két részre bontottuk és

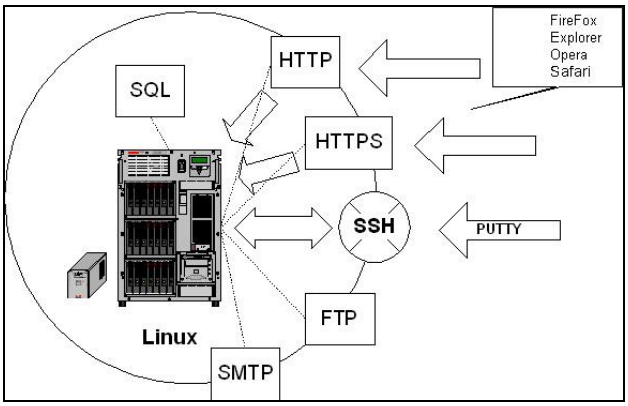
11 Uniform Resource Locator- Webcím

- Perl szkriptet (service.cgi) írtunk, amely - CGI-n keresztül - bináris programot képes futtatni webszerver segítségével;
- elkészítettük a parancssori argumentumokkal vezérelhető, SSH indítására, vagy leállítására alkalmas bináris programot (service.bin).

service.cgi	?	→	start/stop	service.bin
www-data	→	sudo	→	root

A sematikus ábrán követhető a szolgáltatás-vezérlés metodikája.

- Először „service.cgi” kerül meghívásra böngésző segítségével, melyet ténylegesen a webszerver futtatója, azaz „www-data” hajt végre;
- Az URL-ben átadott paramétereknek megfelelően döntés születik a szkript végrehajthatóságáról, valamint a végrehajtandó tevékenységről;
- Pozitív elbírálás esetén jogosultság átadás történik „sudo” segítségével, melynek eredményeként „www-data” felhasználó rendszergazdai jogosultsággal hajtja végre „service.bin” programot, a paraméterben átadott (start/stop) értékkel;
- Az SSH szolgáltatás az utasításnak megfelelően elindul, vagy leáll, melyről visszajelzés érkezik a böngészőben.



1. ábra: SSH vezérlése HTTP(S)-n keresztül
Forrás: Saját

A megoldással elértük célunkat, az SSH szolgáltatást feleslegesen nem működtetük, azonban ha szükség van rá, egyszerűen böngészőn keresztül elindítjuk. Egyedüli problémát a webszerverre irányuló kiszolgáltatottság jelenti, mert annak leállása esetén megszűnik az SSH indítási lehetősége. A bizonytalanságot a webszerver duplikált működtetésével oldottuk meg, külön üzemeltettük a HTTP és a HTTPS kiszolgálókat, így bármelyik kiesése esetén a másik még biztosítja az SSH indítását. A szolgáltatások egyszerre történő leállására kicsi az esély, amennyiben mégis bekövetkezne, akkor vélhetően komolyabb a probléma, a szerverhez fizikai hozzáférés szükséges.

Figyelő scriptek futtatása

A belső hálózatban működtetett Linux szerverek üzemeltetése közben, gyakran felmerült a kérdés bennünk, hogy miként lehetne reagálni egy - esetleges - illetéktelen bejelentkezésre? A költői kérdésre válaszul írtunk egy szkriptet, mely véleményünk szerint egy lehetséges megoldása a problémának. Abból a feltételezésből indultunk ki, hogy a szerverre a hálózaton

csak és kizárólag saját laptopról, vagy pedig a szerverszobában konzolról jelentkezek be, amiből egyenesen következik, hogy amennyiben bármely bejelentkezéshez tartozó IP cím nem a laptopé, akkor az illetéktelen jelenlétre utal.

Másik kiindulópontként két lépcsőssé tettük, azaz letiltottuk a – hálózati – direkt rendszeradminisztrátori bejelentkezést, tehát bárki csak és kizárólag normál felhasználóból válhat adminisztrátorrá. Miután a betörő is csak két lépésben lehet rendszergazda, amely jogosultság megszerzéséhez biztosan némi idő kell, egy rövid ellenőrzés – percenkénti automatizált – végrehajtásában gondolkoztunk.

A szkript algoritmikus működése:

- a rendszerbe bejelentkezett felhasználókhoz tartozó IP címek lekérdezése;
- az IP címek vizsgálata, hogy megegyezik-e a notebooké-val;
- eltérés esetén illegális bejelentkezés történt:
    a) azonnali beavatkozás, hálózati kapcsolatok zárása;
    b) naplóállomány készítése időbélyeggel és a lekérdezett IP címekkel.

A program rövid, alacsony az erőforrás igénye, a betörőnek pedig összesen egy perc áll rendelkezésére, hogy megpróbáljon „root” felhasználóvá válni. Egyik mit sem sejtő kollegánk egyszer megpróbált bejelentkezni, és „azonnal” a szkript áldozatává vált. Ez, és ehhez hasonló megoldások sikeresen alkalmazhatók Linux-ból épített tűzfalakon, routereken is, melyek véleményünk szerint nagyban növelik a védendő hálózat biztonságát.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A mai rohanó világban kulcsfontosságú szerepük van a kritikus információs infrastruktúráknak, melyek működése nélkül egyszerűen megállna az élet. Még belegondolni is borzongató mi lenne, ha a védelmi szféra, a bankok és egyéb intézmények informatikai rendszerei üzemképtelenné válnának, vagy a telefonszolgáltatók szerverei megállnának.

Az említett kritikus információs infrastruktúrák azonban mára teljes mértékben az Internet részévé váltak Az internetes elérésből pedig egyenesen következik a támadhatóság, a próbálkozás, valamint a kiberbűnözők felbukkanása. A háttérben megjelenő adat- és pénztömegek csábító hatása „szakértő-bűnözői” csoportok kialakulását és szervezett támadások összehangolását dimenzionálják. A hatékony védekezés szükségessége megkérdőjelezhetetlen, melyben az oktatásnak, az elfogulatlan tájékoztatásnak, valamint a védelmi szakértők alkalmazásának egyaránt nagy szerepe van.

FELHASZNÁLT IRODALOM

[1] Pulai András, Sziklássy Fábián, Tóth Péter, Udvaros H. Vilmos : Védd magad az Interneten – Kossuth Kiadó Rt., 1997

[2] Brian W. Kernighan - Dennis M. Ritchie : A C programozási nyelv, Budapest, Műszaki Kiadó, 1994

[3] László József : Dinamikus weboldalak, CGI programozás

[4] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal)

[5] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal)

[6] Négyesi Imre: Az információgyűjtés jövőképe (Hadtudományi szemle on-line, I. évfolyam (2008) 3. szám, 95-100. oldal)

[7] Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője (MK KBH Szakmai Szemle 2009. 3. szám, 35-50. oldal, ISSN 1785-1181)

[8] Négyesi Imre: Az önkormányzatok informatikai stratégiája és a Magyar Információs Társadalom Stratégia összefüggései (Hadtudományi szemle on-line, II. évfolyam (2009) 2. szám, 85-92. oldal HU ISSN 2060-0437)

[9] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia előadás, 2010.03.05.-06.)

[10] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05.-06.)

Pölcz Péter – Pándi Erik – Pándi Balázs
ppolcz@codel.hu – pandi.erik@zmne.hu – balazs.pandi@gw.com

AZ INFORMÁCIÓ BIZTONSÁGÁNAK MEGVALÓSÍTÁSI LEHETŐSÉGEI[1]

Absztrakt

Jelen közlemény a biztonság megvalósíthatóságának egyes problematikáját tárja fel.

This publication investigates some of the problems related to possible implementations of Information Security.

Kulcsszavak: *IT biztonság, kriptográfia ~ IT security, cryptography*

BEVEZETÉS

Az információbiztonság napjainkban dinamikus fejlődés előtt áll. Érdekes a fejlesztések és információvédelmi rendszerek tervezésében kialakult állami érdekek és szerepek különbözősége, egyes államok a fejlesztést ipari és iparági alapokon végeztetik, míg más államok teljesen állami irányítás és felügyelet alatt (az elsőre példa a kapitalizálódott államok, míg a másodikra a szocialista és szocializmus alapján szerveződött államok) tervezik a jövő technikáit.

1. MEGVALÓSÍTÁSI LEHETŐSÉGEK NAPJAINKBAN

A nemzetközi elfogadottság szerint (eltérően a magyar viszonyoktól) a szigorúan védett és titkos információk szintjén kezelendő

- maga a minősített információ;
- a tárolás helyszíne;
- a hozzáférő személyek adatai;
- a tárolás és közvetítés során felhasznált kriptográfiai algoritmusok.

Fentiek mellett a védelem másik oldalának eszközei kereskedelmi forgalomban (igaz, ellenőrzött módon) megkaphatók, ezek:

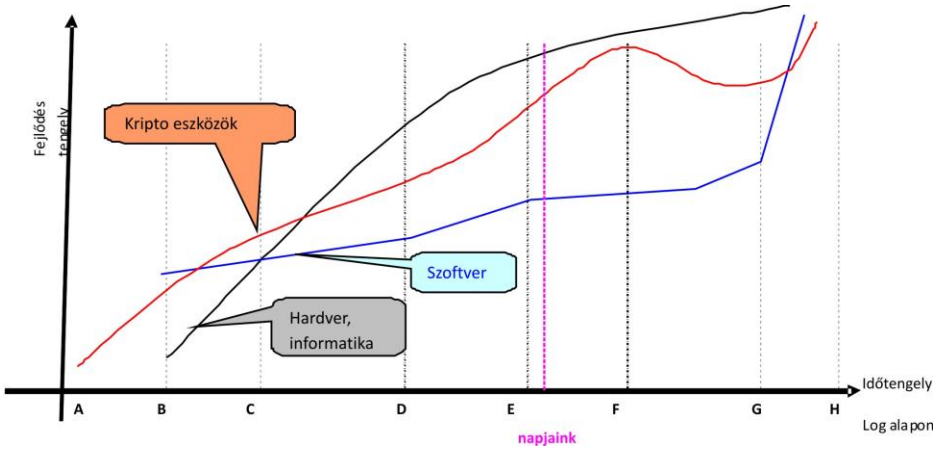
- a rejtjelző eszközök;
- a rejtjelző eszközökön futtatható kriptográfiai algoritmusok (3DES, AES alapokon);
- a rejtjelző eszközök központi menedzselését lehetővé tevő szoftverek és algoritmusok.

A kettős megkülönböztetés célja a rendszer biztonsági tűréseinek behatárolása és ellenőrzése. Ennek oka a már felvázolt kettőségben van, mégpedig abban, hogy az információ a fontos.

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

Jelenlegi technológiai fejlődés mellett a napjaink védett (kriptált információi) minden nap elteltével egyre sebezhetőek, és feltörhetőek. E helyen említenénk meg a következő informatikai fejlődést leíró állapotokat:

- Moore törvényét, melyet a mai napig alkalmazni lehet az informatikai eszközök fejlődésének leírására, mely szerint a processzorok száma (és ezzel együtt a számítási teljesítmény) másfél évente megduplázódik;
- egy Amsterdamban tartott (2006) nemzetközi informatikai konferencián a következő egységes vélemény hangzott el:
  - az informatikai eszközök (számítógépek) elvi amortizációs ideje (míg az újabb technológia megjelenni, másként a technológiaváltás időtartama) 3 hónap;
  - az informatikai eszközök hardver oldali képességei körülbelül a 1GHz-processzor sebesség tartományt átlépve, már magasabb, mint az alkalmazott szoftverek igényei (kivételkén, mint jól alkalmazkodó szoftvert a játékszoftvereket hozták fel, ezzel együtt megítélésünk szerint a szimulációs szoftverek fejlődése az, ami követi a folyamatot), fokozatosan elmaradnak a hardver adta lehetőségektől. Másként a HW-SW olló nyílik és a kinyílás még napjainkban is tart, annak ellenére, hogy az operációs rendszerekben a Microsoft egyre bonyolultabb, de rendszerében nem újabb operációs szoftvereket fejleszt;
  - A szoftver-hardver olló záródására csak komoly technológiai áttörés után lehet számítani, ilyen például a beszéd-, bioszenzor- alapú irányítás és kommunikáció a számítógépekkel. Ezen technológia fejlődése még eléggé visszafogott, de tervezésük az iparágon belül már megindult.



1. ábra

Fenti ábra magyarázata:

- „A” ponttól a „B” pontig a kriptográfiai eszközök IT támogatás nélkül fejlődtek. Gyorsulás a folyamatban az elektronika megjelenésével kezdődött;
- „”B” és „C” pont között az informatika megjelent és ösztönzőleg gyorsította a kriptográfiát, ennek okai a törési idők csökkenése az elektronikai integráció növekedése. („C” pont a HW-SW olló töve az 1 GHz-s processzor sebesség tartomány);

- a „C” és „D” pont a kriptográfiai eszközökben az algoritmusok fejlődését jelentette, ennek lehetőségét a gyors HW eszközök adta lehetőségek hordozták;
- „D” és „E” pont közt a kriptográfia a határokat látva elindul a kvantum kriptográfia felé, megjelennek az első tanulmányok és elvi leírások. A HW-SW olló tovább nyílik, a HW technológia eléri a 0,35 nm szeletnagyságot és az 1 milliárd integrált tranzisztorszámot processzor csippen belül. A SW módosulások még mindig a kezdeti rendszer finomításai és megjelenési modifikációi. Elindulnak a kvantum számítógép fejlesztések és tesztek, megjelennek az első idegi interfészek;
- „F” pontban a kriptográfia jelenlegi formái és technológiái kimerülnek és megjelennek az új technológiák (kvantumtitkosítás és kvantális rendszerek);
- „G” pontban várhatóan bekövetkezik az áttörés az idegi és verbális alapú számítógép vezérlés megvalósításával, ezzel a hagyományos kriptográfiai technológiának vége, új korszak kezdődik az IT és adatfeldolgozás terén. Az új technológiák és technikák, képességei egy az atombomba feltalálásához fogható technológiai forradalomhoz és esetleges nemzetközi feszültségek kialakulásához vezetnek. A kriptográfia új utakra vált ennek alapjai már a kvantumtitkosítás és mellette az általunk „fátyol2” védelemnek nevezett módszerek kifejlesztése jelentheti.

Ha megnézünk egy, a jelenleg kifejlesztés és leírás alatt lévő egyik protokollt a BB84-t (forrás JATE Informatika), akkor láthatóvá válik, hogy a kriptográfia kvantum megközelítése, mint rejtjelzési módszer jó irány, de nem szabad elfelejteni, hogy átviteli sebesség és a leírást létrehozó rendszerek bonyolultsága sem. Amennyiben majdan a kvantum informatikai rendszereket összekötik a bioszenzoros módszerekkel, akkor az emberi agy deduktív képessége és a kvantum számítógép sebessége, adatmanipulációs képessége komoly kihívásokat jelenthet a jövő kódtörői számára.

2. KVANTUM KRIPTOGRÁFIA ÉS A BB84 PROTOKOLL

A két fél: Aliz (A) és Bob (B) üzenetei nyilvánosak lehetnek, de a kódoláshoz és a visszafejtéshez titkos kulcsot használnak, amelyet csak _k ismernek. A kvantumos módszer valójában a titkos kulcs átviteléhez szükséges A és B között, ezért a módszert kvantumos kulcstovábbításnak (vagy kulcs-szétosztásnak) szokás nevezni. Az angol quantum key distribution szavak rövidítéseként QKD módszerről illetve protokollról is szoktak beszélni. A kulcsot mint megfelelő qubitek sorozatát juttatják el egymáshoz, így ha azokon egy harmadik, illetéktelen személy, mérést hajtana végre, akkor elrontja az eredeti állapotot, amit a két fél statisztikai módszerek alapján észre tud venni. Az első QKD protokoll, a BB84-nek nevezett módszer, amelyet C. Bennett és Brassard javasolt 1984-ben. Ez két nem ortogonális állapotot használ a kód előállítására. A BB84 a következőképpen működik. A előállít egy klasszikus véletlen bitsorozatot, melynek k-adik tagja legyen a_k. Ennek a bitsorozatnak egy alkalmas részsorozata lesz majd a titkos kulcs. Ezt fogja A kódolni egy |φk > kvantumálapot sorozattal, amelyek egy kétdimenziós tér elemei.

Ezeket a klasszikus bitekkel szemben kvantumos biteknek qubiteknek szokás nevezni. A kódolás módjának meghatározásához egy másik véletlen klasszikus bitsorozatot a’$_k$ -t

2 „fátyol” védelem a kvantum titkosítás azon formáját kezeli, hogy a normál kvantumtitkosítás visszafejtésekor a kvantum gépek által generáltan a létező összes megoldás egyidejű jelenlétét szűrő szoftver algoritmusok megtévesztése és az információ előlük való elrejtése lesz a feladat. Másképpen fogalmazva, ha a kvantumszámítógépek lehetővé teszik, hogy a „Scrödinger macskája” effektus szerint akár az információ a macska is láthatóvá váljon ezt elkerülendő a kettős védelem , fátylat „teszünk a macskára” azaz kettős védelembe helyezzük adatainkat ezzel a kereséséi szabadságot az egyidejüleg rendelkezésre álló információs mennyiségből a nullára lehetséges csökkenteni. A felfedés és egyidejű és egyszeri rendelkezésre állás estében a fátyol eltakarja vagy kevésbé értékelhetővé teszi az alatta lévő dolgot, információt.

használ a következőképpen: a_k-t attól függően kódolja két különböző bázisban, hogy mi az a'_k értéke. Fizikailag, a tekintett qubiteket fotonok polarizációs állapotainak tekintjük, a jelenleg már kereskedelmi forgalomban is kapható kvantumtitkosító berendezésekben valóban ezeket is használják.

A két bázist a következőképpen választjuk. Az egyiket Z bázisnak nevezzük, amelynek bázisvektorai |↔> és |↕> a horizontálisan, (azaz vízszintesen) illetve vertikálisan (azaz függőlegesen) polarizált foton állapotot jelentik.

Ezeket ortonormáltnak tekinthetjük, mivel <↔ |↕>= 0, <↔|↔>= <↕|↕> = 1. A Z bázis elemei legyenek |↔> vagy |↕> Eszerint, ha a'_k =0, akkor a Z bázist használja, amelynek elemei |↔>vagy |↕> vagyis ha ha a_k = 0 akkor $|\varphi_k>$=|↔> illetve, ha a_k = 1, akkor $|\varphi_k>$= |↕> . Viszont, ha a'_k = 1, akkor az X bázist használja, és ekkor, ha a_k = 0 akkor, $|\varphi_k>$ = |↗ >= $\frac{1}{\sqrt{2}}$ (/↔>+|↕>)=| ↗ > illetve ha a_k _ 1, akkor , $|\varphi_k>$ = |A>= $\frac{1}{\sqrt{2}}$ (/↔>+|↕>)=| ↖> Ezután A átküldi a $|\varphi_k>$ kvantumos véletlen kódsorozatot B-nek, aki mérést hajt végre a $|\varphi_k>$ állapotokon. Mérőberendezését ő is véletlenszerűen állítja be Z vagy X irányba egy általa választott b'_k klasszikus bitsorozat segítségével, ugyanazon előírás szerint mint A. Vagyis, ha b'_k= 0 akkor B is Z irányban mér, míg ha b'_k = 1, akkor X irányban. A mérés eredményétől függően ő is létrehozza saját klasszikus bk bitsorozatát ugyanazon előírás szerint ahogyan A, azaz ha a mérési eredmény a Z beállítás során H, akkor b_k =0, ha V akkor b_k =1, illetve ha a z Világos, hogy ha B éppen véletlenül azonos bázisban mért mint amelyben A kódolt, akkor az eredmény elvileg egységnyi valószínűséggel ugyanaz mint amit A kódolt. Ha viszont B nem azonos bázisban mért, mint amelyben A kódolt, akkor az eredménye csak 1/2 valószínűséggel esik egybe a_k-val. Az alább látható táblázatban összefoglalva láthatók a lehetséges kimenetelek, a táblázat 3-6 sorában a 4–7 oszlopokban a megfelelő mérési valószínűségeket adtuk meg:

	$\|\varphi_k>$	b'_k=0	B'_k=1
		|↔> |↕>	|↗ > | ↖>
a'_k=0 a_k=0	|↔>	1 0	½ ½
a'_k=0 a_k=1	|↕>	0 1	½ ½
a'_k=1 a_k=0	|↗ >	½ ½	1 0
a'_k=1 a_k=1	| ↖>	½ ½	0 1
		b_k=0 b_k=1	b_k=0 b_k=1

1. táblázat

Ezek után B egy nyilvános csatornán közli A-val az ő b'_k sorozatát, de titokban tartja b_k-kat. A most már meg tudja mondani B-nek, hogy melyek voltak ezek közül olyanok, amelyekkel az ő kódolási módja megegyezett, azaz kiválasztják azokat a vesszőtlen elemeket, amelyekre a vesszősek megegyeztek. Látható, hogy ha b'_k =a'_k akkor b_k = ak egységnyi valószínűséggel. Az ezeknek a $_k$-nak megfelelő biteket megtarthatják, mint titkos kulcsot, ekkor ugyanis a kiválasztott a_k-k részhalmaza megegyezik a megfelelő b_k halmazával a másik oldalon. Ha valaki viszont csak a vesszős bitsorozatról szerez tudomást, számára az ak (és b_k-k is) egyforma, azaz ½ valószínűséggel lehetnek 0-k vagy 1-ek . Hiába tudja meg valaki a nyilvános csatorna lehallgatásával a b'_k -k értékét, annak alapján pontosan ½ annak a valószínűsége, hogy ak értéke 0 volt vagy 1, azaz nem jut információhoz.

Valójában azonban A és B nem lehetnek biztosak abban, hogy a két megtartott bitsorozat pontosan azonos, aminek két fő oka lehet. Egyrészt lehetséges, hogy maga a qubiteket átvivő

csatorna nem tökéletes, azaz zajos, másrészt előfordulhat, hogy van egy harmadik személy, aki lehallgatja az átvitt információt. Ezt a személyt E-nek szokás nevezni az angol ”eavesdropper” (hallgatózó) szó miatt. Természetesen E-nek az az érdeke hogy A és B ne vegyék észre, hogy ő lehallgatta az üzenetet. A kvantumos csatorna használata miatt azonban A tudomást szerezhet arról, hogy a csatornát lehallgatják.

Hogy ezt hogyan tehetik meg, az alábbiakban tárgyaljuk. E két módon próbálhat tudomást szerezni arról, hogy milyen $|\varphi_k>$ qubit állapot ment át A és B között. Egy primitív módszer lehet ha E mérést hajt végre a qubiteken. Tudjuk azonban, hogy a kvantummechanikában egy mérés általában befolyásolja az állapotot kivéve, ha E abban a bázisban mér, amelyben A kódolt. Noha E esetleg tudja azt, hogy A melyik két bázisban (az X vagy a Z bázisban) kódolt, mivel ez véletlenszerűen történik, E még e tudás birtokában is átlagosan csak méréseinek felében nem fogja megváltoztatni az eredményt. Maguknak a választott bázisoknak a száma is lehet több stb. Egyébként, ha a kvantumos információátvitel egyes fotonokkal történik a közbeavatkozás nyomán a foton elnyelődik, és meg sem érkezik B-hez.

Egy ravaszabb módszer lehet emiatt, ha E megpróbálja lemásolni az átvitt qubit értékét egy általa külön erre a célra használt kvantumregiszterbe. Meg lehet azonban mutatni, hogy kvantumállapotokat másolni 100 % -os hitelességgel elvileg is lehetetlen. Ez az un. nemklónozhatósági tétel.

Tehát látjuk, hogy vagy a csatorna zajossága miatt vagy E közbeavatkozása miatt az átvitt qubitrendszer megváltozik. Erről A és B oly módon vehet tudomást, hogy föláldozza a megtartott és a közbeavatkozás nélkül biztosan megegyezőnek gondolt bitjeinek egy részét, és ezeket nyilvánosan egyeztetik. Meg lehet mutatni, hogy annak a valószínűsége, hogy a titkosan tartott bitek között nem egyezők vannak arányos a nyilvánosan egyeztetett és eltérőnek talált bitek arányával. Ha ez utóbbi kicsi, tehát a nyilvánosan egyeztetett bitek lényegében megegyeznek a két oldalon, akkor ugyanez igaz a titkosan tartott bitekre is.

Megjegyezzük még, hogy az itt ismertetett BB84 protokollon kívül számos más kvantumos titkosítási protokoll is létezik.

Minden kvantum protokoll az egyszeriség (OTP- one time password) módszerét hordozza fizikai formában. Vélhetően a protokollok és a kvantum teleportálási módszerek változásai miatta az egyszerűség, egyidejűség vélelme az érintetlenség hamis ábrándját fogja jelenteni. Igazabb lesz, mint bármikor Sir Arthur C. Clarke mondása, mely szerint:

„Az ember mindig két nagy ellenféllel küszködött - az Idővel és a Térrel”

3. NEMZETKÖZI LEHETŐSÉGEK

A kriptográfia és az információvédelem mindig is együtt fejlődött és szorosan összetartozó iparágak voltak és lesznek a jövőben is. A hozzáférhető illetve publikált nemzetközi kutatások alapján a következő irányvonalak bontakoznak ki:

- a kriptográfiai eszközök gyorsuló átfutása, azaz elvi amortizációs idejük gyors csökkenése;
- a kriptográfia és a hozzátartozó algoritmusok műszaki átalakulásának és új pályára való lépésének megjelenése;
- az ember mind kódoló és kódfejtő fizikális és mind szorosabb bevitele a rendszerbe.

A kripto eszközök minősítése és a vele futó algoritmusok feltörési biztonságának kipróbálása, illetve a megfelelőségi licencek kiadása lemaradásban van az eszközök műszaki színvonalának gyorsulásához képest. Másik oldalról (információvédelem környezeti oldala), műszaki, illetve fizikai kialakításokat vizsgálva a következő megállapítások tehetők:

- a fizikai környezet kialakítása nem sokban változik;
- a környezeti szabályok és szabályzók változása csak valamiféle poroszos probléma megoldás megközelítés (nem tagadva, időleges megoldásokat adhat, illetve a védelmi rendszerek újabb generációinak megjelenéséig kihúzza az időt a meglévő rendszerekkel);
- az örök probléma az emberi tényező az újabb technológiák megjelenésével egyre komolyabb és mélyebb problémákat vet fel (bioszenzoros interfész nem csak áldás, hanem átok is lehet a védelmi szféra számára).

Amennyiben megvizsgáljuk a napjainkban megjelenő híreket, akkor már körvonalazódik a jövő rendszere és a lehetséges megoldások („csak az ember nem változik", a technika és technológia már rég megelőzte tömegek műszaki felfogásának lehetőségeit). Tekintsük át a következő hírt:

„A fény Albert Einstein által kísérteties távoli hatásként leírt tulajdonságát kutató izraeli tudósoknak sikerült minden eddiginél több - szám szerint öt - foton állapotát összekapcsolniuk.

A Weizmann Intézet fizikusai a Science tudományos magazinban tették közzé tanulmányukat az egyidejűleg két stabil kvantumállapotban létező fotonok előállításáról. A kvantumteleportálásnak nevezett jelenséget szupergyors kvantumszámítógépek készítésére lehet majd használni, igen gyors adatátvitel és feltörhetetlen titkosítás érhető el segítségével.

Jaron Silberberg kutatásvezető a Reuters hírügynökségnek adott interjújában elmondta, hogy jelenleg még komoly akadály van az összekapcsolt kvantumállapotok létének demonstrálása és a gyakorlati alkalmazás között, mert ezek az állapotok igen törékenyek. A fotonok kvantumállapota ugyanis bármely külső beavatkozástól megváltozik.

A kutatócsoport Science-beli tanulmányban rámutatott, hogy korábban három volt a legtöbb foton, amelyeknél sikerült egyidejű összekapcsoltságot igazolni a vizsgálatok során."

Ezen bejelentéseket megelőzően a Svéd Tudományos Akadémia publikálta, hogy sikerült részecskét (fény kvantum részét) klónozni, bár a megoldás jelenleg csak 1, legfeljebb 2 részecskére terjed ki. (Ezen hír mögött a kvantális rendszerek lehallgathatóságát lehet kiolvasni. Ha klónozni tudunk egy kvantum sorozatot, akkor elveszik az a lehetőség, hogy az olvasó (címzett)) észlelje a lehallgatás tényét). Ez a jelen és hamarosan, 10-30 év távlatában a lehetséges és kézzelfogható jövő.

Az információvédelem másik fejlődő ágává válhat a feldolgozó számítógépek lehallgathatóságának és kompromittáló kisugárzás védelmének ismételten fellendülő iparága.

A változások eredményeként várhatóan megjelennek a speciális szoftvereket fejlesztő nagy konzorciumok, valamint a szigorúan elzárt kis alkalmazásfejlesztő nemzeti csoportok. A lehetőségek az új HW technológiákkal párhuzamosan kezdtek kialakulni, de komoly felfutásuk várhatóan az új típusú elektronikák és rendszerek tényleges piacra kerülésével indulnak be.

4. HAZAI LEHETŐSÉGEK

A hazai lehetőségekről, a nemzeti technológiai, szakember és műszaki eszközpark megléte vagy lehetséges (gazdasági lehetőség) kialakítása alapján lehet csak beszélni.

A nemzeti erőforrások és lehetőségek erősen korlátozottak (nincs komoly műszaki –HW-fejlesztő gárda, nincsenek fejlesztő és kutató eszközeink, nincs megfelelő képességünk – tapasztalat és ismeret-), így a magyar lehetőségeket csak az alkalmazásfejlesztésben és rendszerfejlesztésben látjuk. Lehetőségeink még vannak, de amennyiben megalakulnak a nemzetközi szerveződések akkor nemzetgazdaságunk informatikai védelme tartósan leszálló pályára kerül és a nemzeti adat, valamint információvédelmünk teljesen kiszolgáltatottá válik illetve válhat.

Nemzetbiztonsági érdekek és szempontok alapján mielőbb szükség lehet olyan, részben állami tulajdonú fejlesztő és tudásközpontok megalakítására, amelyek alkalmasak információvédelmi alkalmazások terén K+F tevékenység megindítására és eredményes bonyolítására.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Örök kérdés hogy mi a védendő és mi a fontosabb. A védendők körébe helyeznénk magát az információt, adatot, és a védő rejtjelző algoritmust míg, az eszközök maguk korlátozottan védendők, mivel adatot nem tárolnak, a kommunikáció szempontjából transzparensnek tekintendők. Ezen megoldások különböző fejlődési irányokba és sebességekbe terelik az adatvédelem, kriptográfia módjait és rendszerét.

Közleményünkben megállapítottuk, hogy amennyiben majdan a kvantum informatikai rendszereket összekötik a bioszenzoros módszerekkel, akkor az emberi agy deduktív képessége, a kvantum számítógép sebessége és adatmanipulációs képessége komoly kihívásokat jelenthet a jövő kódtörői számára.

A fejlődés nemzetközi és hazai szinten más és más irányokat vett, amelyek alapján elmondható, hogy hazánk e területen napjainkban is versenyhátrányban van.

FELHASZNÁLT IRODALOM:

[1] http://www.sg.hu/cikkek/73231/ensz_konvencio_a_kiberbunozes_ellen

[2] http://www.sg.hu/cikkek/74390/ket_masodpercenkent_jelenik_meg_egy_uj_kartevo

[3] http://www.sg.hu/cikkek/74298/kiberhaboru_helyett_mas_kifejezesek_kellenek

[4] http://www.sg.hu/cikkek/70227/rengeteg_a_bejelentetlen_internetes_buncselekmeny

[5] http://biztonsagportal.hu/premier-elotti-hekkerkedes.html

[6] http://index.hu/gazdasag/vilag/2010/02/02/a_nemet_kormany_ismet_fizet_az_adocsalokat_lebuktato_amde_lopott_adatokert

[7] http://index.hu/tech/net/2010/05/14/a_pentagon_fegyverrel_vagna_vissza_egy_cybertamadasert/

[8] http://index.hu/tudomany/2010/05/14/kvantumteleportalast_mutattak_be_izraeli_tudosok/

[9] http://index.hu/tech/net/2010/05/14/megtalaltak_a_facebook-jelszavak_tolvajat/

Pölcz Péter – Pándi Erik – Pándi Balázs
ppolcz@codel.hu – pandi.erik@zmne.hu – balazs.pandi@gw.com

AZ INFORMÁCIÓ ÉS BIZTONSÁGÁNAK ELMÉLETI KÉRDÉSEI[1]

Absztrakt

Jelen közlemény az információbiztonság elméletével és problematikájával foglalkozik.

This publication deals with the theory of Information Security and problems related to Information Security.

Kulcsszavak: *információbiztonság, az információ értéke ~ IT security, value of information*

BEVEZETÉS

Az információk a tudományos megfogalmazásuk szerint léteztek már az ember megjelenése előtt is, de szerepük az ember megjelenésével kezdődött, aki nem csak, mint tényt, hanem mint a tudás és fejlődés forrását kezelte. Így lett a villámból tűz, a tűz és a fa kombinációjából tűzgyújtás. Az emberi tapasztalás az őskortól felhasználja és asszimilálja a környezetében megjelenő információkat és az azokból levonható következtetéseket és tényeket.

Az ősember tűz megismerése, a zsákmányállatok vonulásának megtapasztalása, az egyiptomiak és maják csillagászati megfigyelései és következtetésein át az ókori görögök matematikai összefüggések felismerésén keresztül a XVIII. XIX század kémiai és mikro szerkezeti illetve atomi felismerésein keresztül eljutunk egy olyan egységes kommunikációs nyelv kifejlődéséhez, aminek alapjait már az ókorban letették, de komolyan használni csak a huszadik század közepén kezdték. Ez pedig a bináris nyelv, ami ma már tudattalanul is beszövi minden napjainkat és fajra, nemre, nemzetre és környezetre ugyanúgy hat, és az emberek többségének ismerete és akaratlagos beszéde nélkül univerzális nyelvvé nőtte ki magát.

Miért kell mégis foglalkoznunk komolyan ezzel a nyelvezettel, amit csak két jel ír le szemben vele a bonyolultnak tűnő kínai nyelvvel? Mert ez az univerzális nyelvezete a világnak. Az univerzalitásából adódóan az általa képviselt kockázata pedig túlhalad minden eddig ismert nyelven és nyelvezeten.

Jelen közleményünkben szeretnénk áttekinteni és elemezni az információ és biztonságának néhány elméleti kérdését.

1. TÖRTÉNELMI ÁTTEKINTÉS

Az ember emberé válásával megjelent a nyelv, majd a számszerűség, és a „beszélt” számszerűség a matematika. Az ember lényéből adódóan a megszerzett információt megosztotta a családjával, törzsével és közösségével, de óvta az ellentől.

Az információvédelem, a megszerzett és értelmezett, vagy értelmezni vélt, adatoknak az elrejtése és szükség esetén az előhívhatósága volt a múltban. Ezen feladatok megvalósíthatóak voltak kezdetben az információ (rajz, kép, jel) elrejtésével, álcázásával

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

elásásával, majd a matematika megjelenésével a puszta fizikai megjelenés helyett a logikai elrejtésekbe és logikai rejtvényekben való közlésekbe történt.

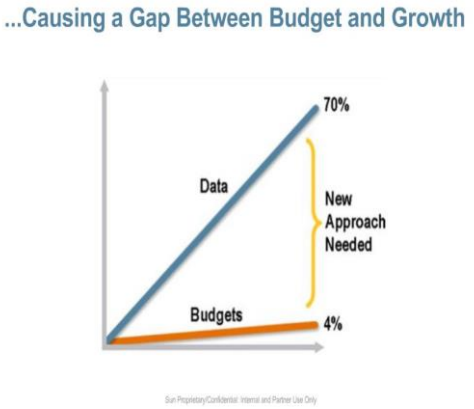
A kezdeti megoldások (kopasz fejre írás, agyagedénybe történő íráson át a görögök kúpos pálcára történő írásán át, az egyszerű cézár kódos adatelrejtésig), egyre komolyabb védelemre váltottak. Ennek okait az információk értékének növekedésében, az tömegesen megjelenő új információk mennyiségében, és maga a „konkurens" felhasználók (ellenséges személyek, majd szolgálatok) mennyiségének növekedésében kell keresni.

Napjaink informatikai rendszerei, korunk exponenciális tudásrobbanásának és az internetnek köszönhetően hatalmas mennyiségű adattal rendelkezik. Ezen információk és adatok tetemes része személyek, cégek, kormányok, államok eredményei és ezért védett információi.

Az kezdeti információ védelemmel szemben most már szabályok, szervezetek és rendszerek védik, vagy próbálják védeni adatainkat, titkainkat.

A védelem erőssége olyan, mint a láncszem, annyit ér, mint a leggyengébb szeme. A kormányok, államok, államközi csoportosulások szabályokat és eljárási rendszereket, módszereket vezettek és vezetnek be az információik védelmére az egyik oldalon, míg ugyan úgy kíváncsiak a másik fél adataira.

Az információ mennyiségének növekedése jóval meghaladja a rá fordított költségek növekedését:



1. ábra

2. JELENLEGI HELYZET

Az információbiztonság mára már egy összetett tevékenység, amely az információt, mint burok körülveszi.

A biztonság alapja a legkülső védelmet jelentő szabályzók és törvények összessége, melyek jogalapot és iránymutatást adnak a védelem megszervezésére és a védendő adatok típusainak meghatározására.

A héj, következő rétege a szervezetekre és ezen belül a végrehajtókra, felhasználókra és kezelőkre lebontott személyügyi biztonság, szabályok kialakítása.

2. ábra

A következő réteg (a harmadik), a környezeti biztonságot megvalósító fizikai eszközök és rétege, mely lehetővé teszi a megbízható környezet kialakítását.

A fent említett rétegek által fizikailag és logikailag körbezárva van az adatkezelés és adatmozgatás, adattárolás szintje mely a tényleges és védett információ kezelését, bizalmasságát és rendelkezésre állását, módosíthatatlanságát, és hozzáférhetőségét biztosítja.

A mellékelt 2. ábrán foglaltuk össze az információ rétegződését és a biztonság kialakításának jogszabályi elvárását.

Az információvédelem másik aspektusa a személyi adatvédelemtől a közösségin keresztül a nemzetiig, illetve a nemzetközi szintekig terjed.

A 3. ábra mutatja be a biztonság személyi, nemzeti, nemzetközi részeit és felületeit.

3. ábra

A védelmi rendszerek és nemzetközi kapcsolatok alapjai ma már az informatikai kommunikáció, valamint a védett információk áramlásának nemzetközi kapcsolatai.

Mindezen tények napjaink pénzügyi és gazdasági mozgatórugójává vált. Ezen tények kihívások a nemzetközi terrorizmus és „fekete” informatikai szakértők azaz hekkerek

számára. A kérdés súlyossága már olyan mértéket öltött, hogy a világ egyik vezető állama az USA már fegyveres válaszreakciókat helyezett kilátásba az ilyen jellegű támadások esetén.

Erre nyíltan felhívta a nemzetközösség figyelmét. Ez természetesen jelenleg csak egy általános megszólítás, de okulva a Lettországot ért kiber támadás példáján már nem lehet szó nélkül elmenni mellette. Ami az alanti idézetet nézve komoly aggodalmakat jelenthet a világ számára mivel ezen támadásokra induló zombi számítógépek áradat akár magán az USA-n belül létezik, vagy akármerre a világban, mivel az internetes összeköttetésből nem minden esetben lehet a támadást indító szervert visszakövetni. Ha a támadó megbújhat a felhőben, vagy esetleg a támadást, mint tényt jelenti be egy állam akkor akár „mondvacsinált" támadási és beavatkozási jogalapot generál az általa kiválasztott állammal szemben,

A közzétett (megszellőztettet) nyilatkozat a következőképen szól:

„James Miller, amerikai védelmi miniszterhelyettes egy washingtoni konferencián azt mondta, lehetséges, hogy az USA fegyverrel vágna vissza egy esetleges, az országot ért számítógépes támadás után."

Azt, hogy mit minősítene a Pentagon az ország elleni kiberháborús támadásnak, az nem derült ki. Ezek jogi kérdések, és nagyon sok homályos részlet van még, amit tisztázni kell ezen a területen - tért ki a válasz elől a miniszterhelyettes.

Az amerikai kormányhivatalok rendszereit érő támadások az utóbbi években, mennyiségben is megszaporodtak, és egyre kifinomultabbak is lettek. A szigorúan védett hálózatokba napi ezres nagyságrendben próbálnak betörni. A támadások mögött állhatnak amatőr hackerek, akik a szakértelmük határait próbálgatják, de bűnözők, terroristák, vagy más országok kémei is. Csak a védelmi minisztériumban hétmillió számítógép dolgozik."

Ezen koncepciók és lehetséges okok keresése eszembe jutatják Eötvös József mondását mely szerint

„Iparkodjál látni! Bekötött szemmel senki sem járhat egyenesen."

A probléma fontosságát és kezelését jelenti, hogy az ENSZ is napirendi pontjára tűzi a kiberbiztonságot.

Az új dokumentum elfogadása az Egyesült Nemzetek Szervezete következő konferenciájának egyik legfontosabb napirendi pontja lehet. Az európai szabályozást terjesztenék ki az egész világra.

Az ENSZ a következő hetekben dönthet a Kiberbűnözés Elleni Konvencióról. Az Európa Tanács aláírói áprilisban az Octopus Konferencián ülnek közös asztalhoz a nemzetközi szakértőkkel, hogy számos témát megvitassanak. Bár az új egyezmény hivatalosan nem szerepel a rendezvény napirendi pontjai között, mégis aligha hagyják majd ki a témák közül. Az ENSZ Drog- és Bűnözés Ellenes Irodája (UNODC) azt javasolta, hogy az online bűnözés visszaszorításáért egy globális szerződést kössenek egymással a világszervezet tagállamai.

Az Egyesült Nemzetek Szervezete áprilisban rendezi meg a 12. Bűnözés Elleni Konferenciáját és az új konvenció kidolgozásának ötletét korábban már négy regionális értekezlet résztvevői is támogatták. Különösen a latin-amerikai országok karolták fel az elképzelést, amelyek álláspontja szerint: "az internetes bűnözés ellen elengedhetetlenül szükség van egy nemzetközi megállapodásra". Ázsia, Afrika és az arab világ szintén támogatásukról biztosították az ötletet.

Az elképzelés nem új keletű, már 2000-ben felmerült egy kiberbűnözés elleni ENSZ konvenció kidolgozása és elfogadtatása. A Global Cybersecurity Agenda keretében a Nemzetközi Távközlési Unió (ITU) is szorgalmazta egy ilyen szerződés kidolgozását. Hamadoum Touré, az ITU főtitkára többször is elutasította azt a javaslatot, hogy az Európa Tanács hasonló konvencióját terjesszék ki az egész világra. Thorbjorn Jagland, az Európa Tanács főtitkára szintén azt kérdezte az ENSZ vezetőitől, hogy miért jobb éveken át energiákat befektetni egy új megállapodás részleteinek megvitatására, mint csatlakozni egy meglévő egyezményhez.

"Jóval hatékonyabb valami olyasmit átvenni, ami már létezik, mint 5-6 éven át egy új dologgal kísérletezni" - szögezte le Alexander Seger, az Európa Tanács gazdasági bűnözés elleni részlegének vezetője is. Az UNODC ugyan elismerte, hogy az Európa Tanács Konvenciójának hatásai jóval túlmutatnak az eredeti célokon, azonban rámutatott arra, hogy sok ország nem hajlandó aláírni egy olyan szerződést, amelynek kidolgozásában nem vett részt.

Az Európa Tanács Kiberbűnözés Elleni Konvencióját eddig 24 ország ratifikálta. Magyarország 2001. november 23-án írta alá a dokumentumot, amit az Országgyűlés 2003. december 4-én ratifikált. A szerződés aláírói vállalják, hogy közösen lépnek fel a gyermekpornográfia, a szerzői jogsértések és a számítógépes rendszerek elleni támadásokkal

2.1. Az információ, mint érték

Mint minden értékkel rendelkezik valakinek. Ezért van az, hogy az állam, mint a csoportos együttműködő közösségek legmagasabb szintje rendelkezik a csoportok értékeinek összességével.

Az értékek beárazódására példa a következő hekker ajánlat:

„http://index.hu/tech/net/2010/05/14/megtalaltak_a_facebook-jelszavak_tolvajat/

2010. május 14., péntek 16:18 | Frissítve: 2010. május 14.

Április végén tűnt fel egy hackerfórumban egy Kirllos nicknevű felhasználó, aki Facebook-felhasználók azonosítóit és jelszavait árulta, méghozzá másfél millió párat.

Az ügyben vizsgálatot indított a Facebook, és a Computerworld értesülései szerint nemrég sikerült azonosítaniuk az elkövetőt, aki viszonylag olcsón árulta az adatokat (25-45 dollárért kínált ezer darabot).

Ha állami adatokról van szó a piaci árazás is változik.

„A német pénzügyminiszter zöld jelzést adott az állítólagos németországi adócsalókat leleplező, lopott svájci banki adatokat tartalmazó DVD-lemez megvásárlására. Két éve hasonlóan döntött a kabinet, akkor a német posta vezére volt az egyik lebukott adócsaló.

Egy informátor a múlt hét végén 2,5 millió euróért ajánlotta fel a lemezt a német államnak. A DVD 1500, svájci bankszámlával rendelkező állítólagos német adócsaló adatait tartalmazza. Az informátor - akinek állampolgárságát hivatalosan nem közölték - előzetesen öt számlatulajdonos adatait rendelkezésre bocsátotta, és a hatóságok minden esetben megállapították az elkövetett adócsalást.”

http://index.hu/gazdasag/vilag/2010/02/02/a_nemet_kormany_ismet_fizet_az_adocsalokat_lebuktato_amde_lopott_adatokert/

Az árak még ennél is magasabbra szöknek ha, ezen adatok és információk az állam működését és működés közben felhasznált, megszerzett információit érint. Ezen kategóriák már a komoly nemzetközi hírszerzés és elhárítás kategóriája.

Így juthatunk el a piacgazdaság és beárazódás kérdéseihez. Eddigi ismereteink szerint a legegyszerűbben, de jól követhetően a Markowitz féle CAPAM modell szemlélteti és mutatja be. A CAPAM modell alapja, hogy 3 féle személy illetve tulajdonos létezik, ezek pedig:

- A kockáztató (szerencsejátékos);
- A közömbös;
- A megfontolt („aki nem játszik dupla vagy semmi játékot”).

Ha a fenti besorolást tekintjük az állam, mint információtulajdonos a megfontolt körbe tartozik, ez alapján a (a szimulált és tapasztalati) piaci megnyilvánulását az alábbi képletekkel lehet leírni. A formula érdekességének tekintjük, hogy az államkockázat szintje magára az államra is vonatkoztatható, és mint így megkaphatjuk azon módosító tényezőket, amelyek az állami információk biztonságának és kezelésének képletét adja.

$$Információbiztonság\_kockázata = Országkockázat \frac{\sigma_{Cégbiztonság}}{\sigma_{\text{Állami minőinősít adatok}}}$$

1. képlet

A piaci beárazódások két fontos tényezője az $E_{(r)}$ ami a hasznosság, tehát az információ fontosság illetve érték kifejezője, míg a $\sigma_{(r)}$ a érték illetve mennyiség kérdése, de az információbiztonság szempontjából, mint adatmennyiség jelenik meg. Tehát azt mondhatjuk, hogy az adatmennyiség és a hozzá tartozó hasznosság (érték) lapján a megfontolt kockázatkerülő formulát használva Markowitz képlet és grafikon a következő táblázatban felsorolt piaci paraméterekkel jeleníthető meg.

Kockázati értékek különböző piacokon		
Piac általános jellemzői	**Példák**	**Kockázati mérték**
Kibontakozó piacok jelentősebb politikai kockázattal	Dél-amerikai piacok, Kína, Oroszország	8-11 %
Kibontakozó piacok kis politikai kockázattal	Szingapúr, Malaysia, Tájföld, kelet-európai piacok	7-10 %
Fejlett piacok széles spektrummal	USA, Japán, U.K.,	5-7 %
Fejlett piacok kevés, stabil vállalattal	Németország, Franciaország	3-5 %

1. táblázat

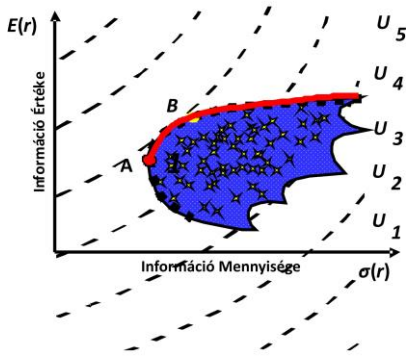
Az információbiztonság és az államinformációs biztonsági kockázat számításakor a fenti táblázat százalékos értékeinek egész számú mértékét véve lehetne a besorolás kockázati tényezőit megadni. Másként a fejlett piacok (vagy másik jó megközelítés a 2. táblázat kockázati értékei, mivel ezen besorolások felülvizsgálata rendszeres), információbiztonsága is fejlettebb mind például a kibontakozó piacok értékei.

Tehát a mellékelten felírt 1. képlet ország kockázati besorolása az 1. vagy 2. táblázat egész számú értékeit veszi fel. A nevezett képlet további változóit a Markowitz féle hasznossági görbék alapján tudjuk meghatározni, oly módon hogy a $\sigma_{(cég)}$ és a $\sigma_{(állam)}$ értékeit a 2. képlet alapján tudjuk kiszámolni. A fenti kockázati értékek mellett jobb híján az államok besorolására mérőértékként a pénzpiaci és államkockázati nemzetközi minősítési alapokat figyelembe véve a következő módosító értékek lehetnek.

Ország	Minősítés	Megszegési kockázat okozta többlet %-ban
Bulgária	**B2**	**5,50**
Csehszlovákia	**Baa1**	**1,20**
Dánia	**Aa1**	**0,60**
Görögország	**Baa1**	**1,20**
Lengyelország	**Baa3**	**1,45**
Litvánia	**Ba1**	**2,50**
Magyarország	**Baa1**	**1,20**
Oroszország	**B3**	**6,50**
Románia	**B3**	**6,50**
San Marino	**Aa3**	**0,70**
Svédország	**Aa2**	**0,65**
Szlovákia	**Ba1**	**2,50**
Szlovénia	**A3**	**0,95**

2. táblázat
Markowitz tőkepiaci hasznosság (CAPAM)

A fentiek után a CAPAM grafikon kinézete a következő, (ahol a már jelzetteken kívül az egyes beértékelődő információk (eredeti formában értékpapírok) mennyiségi ($U_{(1-5-n)}$ és megfontolt módon gazdálkodó személy (állam) görbéket szimbolizálja.



4. ábra

A pirossal jelzett felület az ésszerű kockázatvállalás felülete, másként az információ biztosi tás és biztonság számolható optimális értéke (ráfordítás és értékarány). A táblázatban szereplő U_{1-5} az egyes információk értékelődési rendszere és beárazódásai, az $E_{(r)}$ az adott információ mennyiségek $\sigma_{(r)}$ pillanatnyi beárazódásának értékei.

A Markovitz féle tőkepiaci beárazódás CAPAM tervezési képletei szerinti összefüggésekkel az információérték képlet hasonlóságokat mutat, ezért a megítélésünk szerint a beárazódási képlet azonos az adott információk beárazódási képletével. Tehát

$$\lim_{n\to\infty}\sigma(r_P)^2 = \lim_{n\to\infty}\left(\frac{1}{n}\,\mathrm{var}_{átlagos} + \left(1-\frac{1}{n}\right)\mathrm{cov}_{átlagos}\right)$$
$$= \mathrm{cov}_{átlagos} = k_{ij}\sigma(r_i)\sigma(r_j)_{átlagos}$$

2. képlet

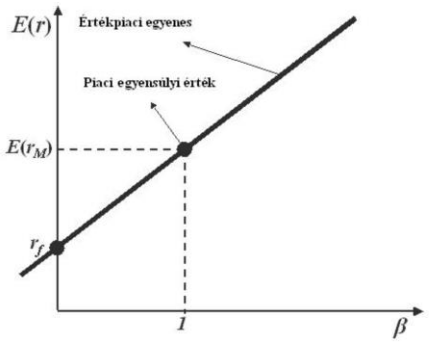
A fenti képlethez tartozó CAPAM egyensúlyi képlete, mely az optimalizációs pont kiszámítását jelenti a következő:

$$E(r) = r_f + \beta\left(E(r_M) - r_f\right)$$

3. képlet

Az A pont a hasznossági alap, a B pont az információ mennyiség (diverzifikált) piaci egyensúlypontja (a tervezési alap).

Az érték piaci egyenes, amely a 4. ábra „B" pontjára és az adott információ számunkra vonatkozó „beszerzési" értékének (E_r) pontjain áthaladó egyenes reprezentálja.



5. ábra

Az összefüggésből látható, az optimalizációs érték az végül is egyenlet β-jától függ. Ezen alapon az információvédelem és összessége a nemzeti kockázat értékével korrelálva mérhető adatokkal szolgáltat az információs érték piaci becslésére, valamint az ebből számítható optimalizált védelemre. (Természetesen lehetnek az optimalizálttól eltérő kialakítások is, olyan helyeken ahol az információ értékeket nem diverzifikáltan kezeljük, hanem egyéb megfontolások szerinti védelmi biztonságokat alakítunk ki. Ilyen területek például a hírszerző és elhárító területek.)

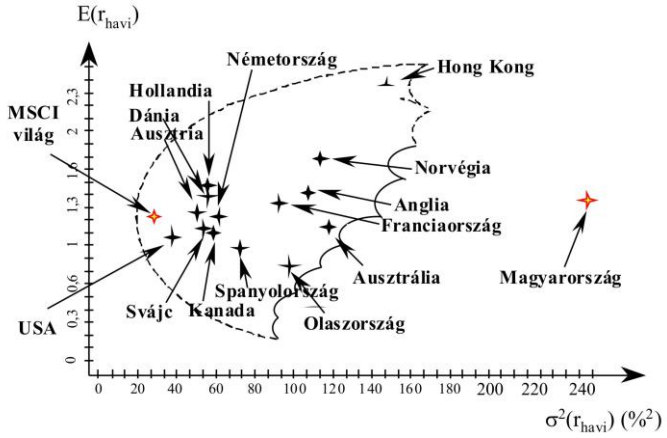
A fenti képletek mellett a tőkepiaci mutatókat a következő táblázat tükrözi, mivel a tőkepiaci kockázatok szintjei között összefüggéseket vélek az információpiaci értékek és árazódások között, ezért a mellékelt táblázat vélelmezésünk szerint következtetési alapként szolgálhat az információ piaci értékének és az ebből adódó védelmi költségeinek a megfogalmazására. (a táblázatot mindig az épen időszerű piaci minősítések és besorolások szerint aktualizálni kell).

Ha most az előző értékek szerint összeállítjuk a nemzetek információbiztonsági kockázattérképét, akkor megkapjuk a nemzetközi mérhetőségi és beértékelődési diagramot vagy táblázatot (6. ábra)

A 6. ábra jelenleg az információértékek (beszerzési, védelmi) hiánya miatt, jelenleg csak a piaci beárazódás és kockázati szintek alapján készült, alapvetően a tőkepiaci besorolások eredményeivel. Az ábra mindenesetre így is jól illusztrálja a fejlett piacok és gazdaságok

besorolási rendszerét, valamint az információbiztonság kockázati értékét. Magyarországi besorolás meglehetősen kockázatos kategóriába esik, ennek okai:

- Gazdasági helyzet;
- Politikai stabilitás kérdése;
- Az információkezelés rendszereinek szabályozatlansága;
- Tőkeerő hiány;
- Személyi, emberi elkötelezettség alacsony színvonala.



6. ábra

A fenti kockázatok és piaci beértékelődések szerint ezek alapján számszerűsíthetően meghatározható az egyes államok információbiztonsági értéke, valamint az információvédelemre fordítandó optimális (már ha lehet ilyenről beszélni) pénzbeli költség, melyet csak rendkívüli estekben kellene túllépni.

2.2. Az információ, mint üzlet és üzletág

Anatol France szerint: „Az ostobaság akkor is ostobaság marad, ha harminchatmillió száj ismétli”

A közvéleményben él az a megközelítés, hogy személyes adatok piaci beértékelődése alacsony. Ezen állításukat azon tényekkel támasztják alá, hogy személyi adataikat mindenütt elkérik, és szükséges az ügyintézéshez. Sajnos ezen állítás részben igaz is mivel a jelenlegi (és itt most magyarországi viszonyokat nézünk), rendszer nem teszi lehetővé a személyi adatok védelmét.

Például nem tudunk mobil telefont vásárolni, vagy nem léphetünk be egy épületbe, esetleg egészségünk miatt kórházba kell menni vagy orvosi ellátás szükséges, oda kell, hogy adjuk személy igazolványunkat, lakcím kártyánkat, közel minden személyi adatunkat. Az adataink kiszolgáltatottá válnak, nem tudjuk azok felhasználását ellenőrizni, biztonságáról illetve biztonságos kezeléséről meggyőződni. Sajnos csak sejtéseink lehetnek a kiszolgáltatott adatok biztonságáról, mikor például, a telefonvásárlás után megkeresnek különböző cégek mindenfajta „személyre szabott” ajánlattal.

A személyi adatok birtokában az adott emberről, környezetéről, rokonságáról, egészségi állapotáról szinte mindent megtudhatunk. Az előzőekben említett hekker aki árúba bocsájtotta a megszerzett információkat 25-45 USD áron kínált ezer darab személyes belépő adatot, ez 0,025-0,045 cent/ darab, ami jelenlegi áron 5,5 Ft- 10,1 Ft/db árat jelent. Ez egy érdekes piaci beértékelődés. Minden bizonnyal az ezer darabból jó, ha egy tovább

felhasználható (banki adatok, belépési adatok stb), de még így is nevetségesen alacsony a személyi adatok és piaci információk beárazódásának módja.

Az állami adatok piaci beárazódása más kategória, mivel ezek értékei a nyilvánosságra kerülésükkel hatalmas károkat okoznak, míg ugyanazon pillanatban devalválódnak. Az állami információk értéke és piaci beértékelődése teljesen hasonló képet mutat, mint a tőzsdepiaci beértékelődés. A tőzsde is reagál a negatív-, a pozitív hírre, leárazódnak vagy felárazódnak egyes részvények. Az állami információk is (legyenek azok akár minősített adatok is) az állam helyzetéből és megnyilvánulásaiból adódóan pénzben kifejezhetően változik. Ha egy olyan gazdaságot veszünk például, mint Görögország, akkor pár évvel ezelőtt hírszerző szervek egyes információkért jóval nagyobb árat kellet, hogy fizessenek (az információ megszerzésének összesített bekerülési ára) mint manapság, mikor a Görög állam a gazdasági problémái miatt is devalválódik.

Az információ tehát pénzben kifejezhető érték és a téves elképzelésekkel ellentétben nem csak elvi értékvonzat van. Az állami adatokat és információkat a tömeg, a konkurencia, a különböző hírszerző szolgálatok, akik az információt tudni, megszerezni vágynak, rajtuk keresztül a piac azonnal beáraz, beértékel („Mennyit ér meg ez neked” tipikus kérdés az értékalap meghatározásakor). Az információk értékmegőrzése mindaddig megvan, míg az információ nyilvánosságra nem kerül, mivel ekkor maga nyilvánosság, tehát a nyílt megszerezhetőség devalválja nullára az addig értékes információt.

A fentiek alapján állíthatjuk, hogy az információ védelme egy piaci értékvédelem, melyet tervezni lehet és kell mind költséget, mind rendszert.

Az információ értéke idővel, hellyel és távolsággal ugyanúgy változik és beértékelődik a „piacon” mint egy kötvény, részvény vagy pakett. (Más értéke van egy Mexikói állami minősített információnak a környező országok számára min például Magyarország számára. Más értéket képvisel 5-10-50-100 év elteltével ugyanazon adat információ, mint aktualitásának és kihatásának idejében. Más értéket piaci értéket képez egy a sivatag közepén lévő törzs részére egy állami információ, mint az éppen elérhető víz értéke, az arányok sokszor nagyon eltérhetnek.) Az értékképzés mindig piaci és mind inkább felfelé haladunk az információs létrán –személy, terület, ország, államszövetségek, ENSZ- a minősített információ beárazódása a kockázat és kihatás alapján egyre gyorsabb és nyilvánosságra kerülési devalvációja is villámsebesen zajlik.

A fenti összefoglalás szerint határozott véleményünk, hogy az információ piaci árazódása azonos és párhuzamos a tőzsdepiaci folyamatokat leíró matematikai modellekkel.

Ezek szerint, ha az információ számban és nagyságban kifejezhető érték, így annak kereskedelme is meg kellett, hogy valósuljon. A megvalósulásának tipikus példája a hekkerek által áruba bocsájtott személyes információk darabárai, a nagy médiacsatornák információigényének kielégítésekor felmerült megszerzési árak, az állami információk eladása illetve megszerzésére fordított más és saját állam által finanszírozott hírszerző tevékenységek és azok költségei.

3. VÁRHATÓ JÖVŐ

Mint ez előzőekben megállapítottuk, hogy az adatok és információk pénzbelien beárazódó értékek, ezért az információéhség kielégítésével növekvő internetes, nemzetközi hálózatok egyre komolyabb támadásokat kezdeményeznek az információk megszerzéséért. Az információ, vagy adatvédelem kulcsai már kezdenek berozsdásodni, mivel a jelenlegi rejtjelzési módszerek a rendelkezésre álló egyre nagyobb informatikai és műveletvégző kapacitás növekedésével mind nagyobb sérülékenységnek vannak kitéve.

A 2010 májusában „Kiberbűnözés - globális veszély?” címmel rendezett berlini konferencián hangzott el (konferencia két fő szervezője a Szövetségi Bűnügyi Hivatal (BKA) és a Szövetségi Információstechnikai Biztonsági Hivatal (BSI):

„Egy jelentés szerint Németországban tavaly 33 százalékkal nőtt az információs és telekommunikációs bűncselekmények száma és elérte az 50 254 ügyet, ez 2008-hoz képest 12 354 esettel többet jelent. 46 százalékos értékével továbbra is a számítógépes csalás és az adathalászat (22 963 eset) a legnépszerűbb IT-bűncselekmény, de szintén kedvelt az adatok elfogása és kikémlelése (11 491 eset), míg a nyomozók 6319 adathamisítás ügyet regisztráltak. 3,1 százalékos értékével a lista közepén található az adatmódosítás/számítógép-szabotázs kategória, tavaly 2276 ilyen esetet jegyeztek fel”

Valamint:

„A bűnügyi rendőrség jelzőszolgálatához 2923 adathalászattal kapcsolatos bejelentés érkezett, ez több mint 64 százalékos növekedés a 2008-as évhez képest. Ezekben az esetekben az átlagos kárösszeg elérte a 4000 eurót.< Regisztráltak még 53 hitelkártya-adatlopást, 617 hozzáférési információ (jelszó stb.) lopást és 3207 telekommunikációs hálózatok használatával szembeni visszaélést. 2009-ben összesen 6800 digitális személyazonosság-lopási ügyre derült fény.

Az elkövetők többsége szervezett bűnözői csoport tagja. Ezek a szervezetek rendkívül profi módon dolgoznak,a tevékenységük nem áll meg az országhatároknál. Jellemző, hogy a hackerek és a vírusírók együttműködnek, valamint elmondható, hogy a kiberbűnözők rendkívül jól és gyorsan alkalmazkodnak a változó technikai környezethez és az átlagosnál jobb innovációs képességük van.”

Mivel világunkra jellemző a globalizáció, így az információkereskedelem (minden irányban, mind a megszerzés, mind az értékesítés) is globalizálódik, ennek részei a hatalmas (ma már milliós nagyságrendet elérő zombi gépek) botnet hálózatok, valamint az interneten megjelenő információk adás vétele és beszerzése is.

A rendszerek természetes fejlődése, az emberi nyitottság és sokszor ostobaság, teszi lehetővé, hogy az úgymond közösségi oldalak legyenek az információszerzés és kereskedelmek központjai.

Az információk nyitott hálózatba való irányítása, a felhőben lévő számítástechnikai teljesítmény exponenciális növekedésével egyre nagyobb kockázatokkal jár.

„Ha a valóságról szerzett tudomásunk kezdete és vége a tapasztalat, mi szerepe van a tudományban az értelemnek?” …..Albert Einstein

3.1. Az információk kereskedelme

Mivel az információ és az adat piaci áron beárazható és automatikusan be is árazódik, ezért ennek kereskedelme és piaci adásvétele is létező folyamat.

Akár az ókorig is visszamehetünk bizonyítékokért, hogy információkat, adatokat vásároltak az ókori államok, személyek, kereskedők. A vásárlás célja előnyszerzés, értékszerzés, gazdasági főlény megszerzése, zsarolás volt.

Az internet új korszakokat nyitott az információáramlásnak, mind a beszerezhető, mind a közvetítői oldalon. Az internet és számítógépes hálózatokat hozzáférhetősége adja az információáramlás exponenciálisan növekvő mennyiségét, és kereskedelmének soha nem látott módjait és lehetőségeit. Ma már az információvédelemnek nem csak a személyekkel és létező szervezetekkel szemben kell védekeznie, hanem egy virtuális térben generált és anonim hírszerzőkkel és kereskedőkkel is. A feladatok komplikáltságát jellemzi, hogy a támadások és információ megszerzési kísérletek már meghatározhatatlan helyről (szélsőséges esetben akár a saját rendszerünkből) indított támadások is lehetnek. A helyzetet jellemzi, hogy a legmagasabb szervezet az ENSZ is a tagállamok részvételével komoly tervezeteket és ajánlásokat készül bevezetni az anonim és egyre terjedő információvadászoktól, információkereskedőktől, a kiberbűnözőktől.

Megemlíthetjük az ENSZ-konvenció tervezet anyagát a kiberbűnözés ellen

„Az Egyesült Nemzetek Szervezete áprilisban rendezi meg a 12. Bűnözés Elleni Konferenciáját és az új konvenció kidolgozásának ötletét korábban már négy regionális értekezlet résztvevői is támogatták. Különösen a latin-amerikai országok karolták fel az elképzelést, amelyek álláspontja szerint: "az internetes bűnözés ellen elengedhetetlenül szükség van egy nemzetközi megállapodásra". Ázsia, Afrika és az arab világ szintén támogatásukról biztosították az ötletet.

Az elképzelés nem új keletű, már 2000-ben felmerült egy kiberbűnözés elleni ENSZ konvenció kidolgozása és elfogadtatása. A Global Cybersecurity Agenda keretében a Nemzetközi Távközlési Unió (ITU) is szorgalmazta egy ilyen szerződés kidolgozását. Hamadoum Touré, az ITU főtitkára többször is elutasította azt a javaslatot, hogy az Európa Tanács hasonló konvencióját terjesszék ki az egész világra. Thorbjorn Jagland, az Európa Tanács főtitkára szintén azt kérdezte az ENSZ vezetőitől, hogy miért jobb éveken át energiákat befektetni egy új megállapodás részleteinek megvitatására, mint csatlakozni egy meglévő egyezményhez.

"Jóval hatékonyabb valami olyasmit átvenni, ami már létezik, mint 5-6 éven át egy új dologgal kísérletezni" - szögezte le Alexander Seger, az Európa Tanács gazdasági bűnözés elleni részlegének vezetője is. Az UNODC ugyan elismerte, hogy az Európa Tanács Konvenciójának hatásai jóval túlmutatnak az eredeti célokon, azonban rámutatott arra, hogy sok ország nem hajlandó aláírni egy olyan szerződést, amelynek kidolgozásában nem vett részt.”

Mindeszek szerint bizton állíthatjuk, hogy az „adatkereskedői”, hírszerző és elhárító tevékenység napjaink komolyan felfutó iparágává válik, akárcsak az adatok és információk védelmének és biztonságos tárolásának, közvetítésének, és szétosztásának ipari méretű rendszerei.

3.2. A megbízható információ közvetítés és módszerek

Hat évtized fejlődésére tekinthetnek vissza a kódfejtők azóta, hogy 1949. októberében megjelent Claude Shannon "A titkosított távközlési rendszerek elmélete" című úttörő tanulmánya. Ez a mű teremtett elsőként szilárd matematikai alapot a kriptográfiának és így a rejtjelezés művészetből tudománnyá vált.

Napjainkban már a mindennapi életben, a GSM-telefonok használata során, webes vásárláskor, vagy filmek és zenék letöltése közben is találkozhatunk a titkosítással - és a hackerekkel, akik nem annyira örülnek a magas szintű biztonságnak.

A titkosítás fejlődése bizonyos értelemben már azelőtt befejeződött, hogy a történet elkezdődött volna: Gilbert Vernam távközlési mérnök és Mauborgne kapitány az első világháború alatt megalkották a tökéletesen biztonságos rejtjelet az amerikai hadsereg számára. Az egyszer használatos, véletlen számokkal teleírt űrlapok vagy lyukszalagok a továbbítani kívánt információval keverve (ún. XOR művelet) feltörhetetlen kimenetet adnak, amit kizárólag a kód birtokában lévő címzett tud elolvasni - feltéve, hogy a számsorokat soha nem használják fel újabb kódoláshoz és az űrlap elkészítéséhez használt véletlenszámok valóban véletlenszerűek.

A gyakorlat és az elmélet nem mindig fedi egymást

A fenti két alapkövetelmény az óta is számos bonyodalom forrása. Bár az OTP rövidítéssel ismert módszer annyira egyszerű, hogy papíron, ceruzával végre lehet hajtani, de nagyon sok kulcsanyagot igényel - ugyanannyit, mint amilyen hosszú az üzenet és ezt nehéz folyamatosan biztosítani. Az ötvenes évek szovjet atomkémei a kulcs-űrlapok újrafelhasználása miatt lepleződtek le, bár ehhez a feltöréshez az amerikai NSA ügynökség elődjének egy évtizeden át kellett dolgoznia a VENONA-terv keretében.

A Wi-Fi vezetéknélküli rádiós hálózatok első változatában alkalmazott titkosítás is az egyszer használatos kulcs egyik változatának tekinthető. Ez a WEP nevű kódolás pár éve azon bukott el, hogy az adatforgalom titkosítására használt RC4 módszer valódi, előregyártott véletlenszámok helyett a chipekben azonnal generálható ún. álvéletlen számsorokat használt. Ezeket utólag elemezni lehetett, a T. J. Maxx áruházlánc bankkártyás vásárlási rendszerébe is így jutottak be 2005-ben a hackerek.

Rossz példát eleget láttak

Az egyszer használatos kulcs fent említett problémái arra ösztönözték Claude Shannont és követőit, hogy - miután 1949-ben bebizonyították a helyesen alkalmazott Vernam-kódolás feltörhetetlenségét - inkább gyakorlatias helyettesítő megoldásokat keressenek a kiváltására.

Ez nehéz feladatnak ígérkezett, mert a kulcs-takarékos titkosító rendszerek a múltban gyenge teljesítményt nyújtottak. Ennek szenvedő alanyai leginkább a németek voltak: az első világháborúba egy feltört mexikói német követségi távirat ismeretében lépett be az USA. A második világháborúban sok német tengeralattjáró veszett oda a híres ENIGMA tárcsás rejtjelező gép üzeneteinek visszafejtése miatt - ezt a munkát a számítástechnika társalapítójaként ismert brit Alan Turing végezte.

Shannon könyve nyomán viszont a civil egyetemi szférában is megindult a kriptográfia kutatása, nem kis részben az IBM cég támogatásának köszönhetően, amely igyekezett az üzleti életben népszerűsíteni a számítógépek használatát. Az első széles körben elterjedt típus, az IBM System/360 megjelenésével a vállalatok hamar igényelni kezdték az elektronikus titkosítást: az 1971-ben megjelent Lucifer rendszert az amerikai NSA lehallgató ügynökség tanácsára továbbfejlesztették és DES néven szabványosították az elektronikus kereskedelemben.

Ez a szimmetrikus titkosító rendszer két évtizeden át szolgálta az informatikát, azonban a kulcsok kezdeti eljuttatása az egymással biztonságosan kommunikálni kívánó felekhez még mindig hálózaton kívüli kapcsolatfelvételt igényelt. A kilencvenes évek közepére a DES-56 elmaradt az egyre gyorsabb chipek fejlődéséhez képest - öt munkanap alatt gyakorlatilag az összes lehetséges kombinációját végig tudta vizsgálni egy negyedmillió dollárból felépített egyedi kódtörő számítógép (ugyanez ma már csak tízezer dollárba kerül).

Erre a problémára az első megoldás a 3DES, a titkosítás oda-vissza-oda alkalmazása volt, amely ma is biztonságos, de igen lassú módszer. 2001-ben végül AES néven az európai Rijmen-Daemen szerzőpáros gyors és takarékos e-siffírjét szabványosították helyette, amely lehetővé teszi, hogy az erős titkosítás akár a legkisebb elektronikus "kütyüben" is megjelenjen.

Színre lép a nyilvános kulcsú titkosítás

Az ilyen széleskörű elterjedésnek, az időközben az egész világot behálózó weben keresztüli használatnak az is előfeltétele volt, hogy kulcscsere kérdését ugyanazon a csatornán, a netkapcsolaton át meg lehessen oldani - küldöncök, faxüzenet vagy hasonló kerülőút nélkül.

Azt az ellentmondást, hogy a titkosítás beindításához szükséges első üzenetet mivel titkosítjuk eredetileg az angol és amerikai hírszerzőknek sikerült feloldaniuk a hatvanas években - a civilek azonban csak Rivest, Shamir és Adleman kutatók 1977-es újrafelfedezése után találkoztak először a nyilvános kulcsú titkosítással.

A módszer lényege az, hogy minden titkosítást igénylő felhasználó készít egy két részből álló, egymással összefüggő kulcspárt, amelyből az egyik szabadon nyilvánosságra hozható és segítségével bárki küldhet a címzettnek olyan védett PGP üzenetet, amelyet illetéktelen harmadik fél nem tud elolvasni, mert a tartalom csak a privát kulcs birtokában dekódolható.

Ezt a rendszert egy matematikai furcsaság teszi működőképessé, ugyanis nagyságrendekkel könnyebb hatalmas számokat szorzással előállítani, mint amennyi idő alatt azokat sorozatos osztással elemi alkotórészeikre, prímszámokra lehet bontani. Bizonyos speciális csoportokra, ahol a prímek óriásiak, ezt feladatot a számítógépek nem is képesek földtörténeti időn belül megoldani, így az ezekre alapozó erős titkosítást biztonságosnak tekintik a kutatók.

Némi aggodalomra adhat okot, hogy a fenti feltevést eddig nem sikerült matematikai szigorúsággal bizonyítani, bár helyességét tízből kilenc kutató biztosra veszi. Ha mégsem úgy lenne és beütne a baj, már készen áll egy alternatív módszer, az ún. elliptikus görbék rendszere, amelyre kicserélhetik a nyilvános kulcsú titkosítás "motorházteteje" alatt rejtőző matematikai apparátust.

Ez a többszörös biztonságot nyújtó rendszer, amely az ezredfordulótól az amerikai export-tilalmi korlátozások feloldásával az egész világon elterjedt, a titkosítás virágkorát hozta el a neten. A fogyasztók könnyedén vásárolhattak akár más földrészen működő boltokból is hitelkártyával, a globális cégek biztonságosan mozgathatták számítógépes termékterveiket egyik üzemből, országból a másikba.

Sokan úgy gondolták, hogy az általános titkosítás (TPM) lehetetlenné teszi majd a számítógépes visszaéléseket, sőt a mindennapi élet teljességét át fogja hatni a védelem, például az összes e-mailt kódolva fogják elküldeni (ún. cipherpunk mozgalom).

Közbeszólt a hacker

Jóslatuk nem következett be, talán mert a szimmetrikus és aszimmetrikus (nyilvános kulcsú) titkosítást kombináló, gyors, olcsó és gyakorlatias módszernek van egy alapvető hátránya: megszűntek a kattogó, berregő rejtjelgépek. A siffrozási munka minden fázisát el tudja végezni maga a számítógép, amely egy általános célú programozható eszköz.

Ezt a jellegzetességet kihasználva a hacker figyelmen kívül hagyhatja a hálózaton átutazó titkosított adatokat és inkább feltöri az egész gépet (operációs rendszert), hogy saját kártékony programját futtatva kinyerje onnan a titkosítás előtt álló, vagy éppen dekódolás után felszabaduló információkat - amelyek a mai világban egyre több pénzt érnek.

Ez hatékony módszer, mert a mai számítógépek operációs rendszerei és program-alkalmazásai nagyon összetettek és bonyolultak, számos biztonsági hibát, rést kínálnak a betöréshez. A legkapzsibb hackerek még azzal is megpróbálkoztak, hogy maguk titkosítsák a feltört gépeken talált adatokat és váltságdíjat követeljenek a felhasználótól a dokumentumok feloldásáért cserében - szerencsére ezeket a kísérleteket eddig még mindig sikerült hatástalanítani.

Tudományos és fantasztikus a titkosítás jövője

Talán a hackerek és kémek problémája hívta életre a titkosítás legújabb, igen bonyolult módszerét. A kvantummechanikai kriptográfia, Bennett és Brassard találmánya az elemi részecskék különös viselkedési módjait használja adatvédelemre: az egyes fotonok (fényrészecskék vagy elemi hullámok) mérése szükségszerűen megváltoztatja azok állapotát, így az egymással kommunikáló felek között elhelyezett lehallgató berendezés nagyon hamar lelepleződik.

Az egymással "mágikus" kapcsolatban maradó, egyszerre keltett elemi részecske párok is felhasználhatók kvantum-számításokhoz - ezek nagy távolságból is azonnal észlelik a másik állapotának megváltozását, mindmáig megoldatlan problémát okozva az elméleti fizikusoknak.

Érdekes megfigyelés, hogy a kvantum-titkosítású adatátvitelben a biztonságos kulcscserét egy BB84 elnevezésű, egyszer használatos kulcsú rejtjellel szokták megoldani. A titkosítás elméletének fejlődése tehát voltaképpen egy nagy kört futott be az évtizedek alatt, magasabb

műszaki színvonalon visszatérve az első világháborúban felfedezett eredeti, feltörhetetlen kódoláshoz.

Azt, hogy a kör a gyakorlatban is bezárul-e, még nem lehet tudni. A kvantum-kriptográfia alkalmazásához a számítógépeket külön optikai hálózati eszközökkel kell kiegészíteni, amelyek legalább 100 ezer dollárba kerülnek. Minden résztvevő páros közé direkt üvegszál kapcsolatot kell kihúzni és cserében szerény, egy otthoni ADSL vonal kapacitásának negyedét kitevő sebességet kapunk, legfeljebb százmérföldes távolságon. A módszert ezért ma csak a hagyományos titkosítás kulcscsere lépése helyett használják, ahol kicsi az adatátviteli igény.

A kémek és hackerek reménykedhetnek, hogy a kvantum-titkosítás még sokáig nem fog túlterjedni a nemzetbiztonság és a nagy bankok falain. Ha mégis, talán jön majd egy zseni, aki összeegyezteti a relativitás-elmélet és a kvantummechanika közötti éles ellentmondásokat - az általa alkotott új elmélet módot adhat a kvantum-viselkedés megjóslására, feltörésére és így a jövő kódfejtői sem maradnak munka nélkül.

Mindezek mellett fel kell hívnunk a figyelmet arra is, hogy az induló kvantum kriptográfia iparág másik oldala a kvantumszámítógépek és kódtörések is dinamikus fejlődésben vannak.

A kvantum kriptográfia mint az adatközvetítés új módszerei szerepelnek, míg a védelem egyéb tényezői, úgymint a tárolás, és szétosztás a már 10-20 éve használt módszerekkel valósul meg. Véleményünk szerint a következő informatikai és adatvédelmi robbanást a biztonságos tárolás és a biztonságos megszemélyesítés köreiből fog kikerülni.

„A tudomány haladását nem az eldöntött, hanem a felvett kérdésekkel kellene mérni”
Eddington

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Napjainkra az információ megtartása, elrejtése és megvédése ugyanolyan üzletággá vált, mint a másik információjának megszerzésére való törekvés. Jelenünkben az adatvédelmi és adatszerzési eszközöket a pillanatról pillanatra változó és növekvő informatikai, számítástechnikai kapacitásban, az emberi szellem, találékonyságában és kreativitásban találhatjuk meg. Mindezeket ma már olyan szavak jellemzik, mint giga- és terrabites optikai hálózatok, űrkommunikációs routerek és switchek, kvantum számítógépek, hacking, social engineering kifejezések.

Közleményünkben megállapítottuk, hogy a tudás, információ értékét mindig a piac árazza be, ezért van az, hogy a személyi adatok értéke alacsonyabb, mint az állami illetve nemzetközi adatok értéke.

A kockázatok és piaci beértékelődések szerint ezek alapján számszerűsíthető és határozható meg az egyes államok információbiztonsági értéke, valamint az információvédelemre fordítandó optimális (már ha lehet ilyenről beszélni) pénzbeli költség, melyet csak rendkívüli estekben kellene túllépni.

Úgy gondoljuk, hogy, ha az információ számban és nagyságban kifejezhető érték, úgy annak kereskedelmének is meg kell valósulnia. A megvalósulásának tipikus példája a hekkerek által áruba bocsátott személyes információk darabárai, a nagy médiacsatornák információigényének kielégítésekor felmerült megszerzési árak, az állami információk eladása, illetve megszerzésére fordított más és saját állam által finanszírozott hírszerző tevékenységek és azok költségei.

Az információkkal való gazdálkodás ugyanakkor megteremtette az információvédelemmel történő foglakozásokat és iparágakat. A technika és tudomány fejlődésével, valamint a tudományos eredmények, vívmányok viszonylag szűk csoportoknak volt elérhető, addig mára ezen rendszereket alkalmazók vagy alkalmazható személyek, csoportok és társaságok köre kibővült a világ lakosságának több mint harminc százalékára.

Ezen lehetőségeket az internet a világháló biztosította és biztosítja a több milliárd felhasználója részére.

A jövőbe tekintve megállapítottuk, hogy a kvantum kriptográfia mint az adatközvetítés új módszerei szerepelnek, míg a védelem egyéb tényezői, úgymint a tárolás, és szétosztás a már 10-20 éve használt módszerekkel valósul meg. Véleményünk szerint a következő informatikai és adatvédelmi robbanást a biztonságos tárolás és a biztonságos megszemélyesítés köreiből fog kikerülni.

FELHASZNÁLT IRODALOM

[1] BME MBA „Vállalati pénzügyek” dr. Andor György (BME 2004)

[2] SUN műszaki és kereskedelmi tréning anyagai 2009

[3] JATE Informatika: Kvantum kriptográfia és a BB84 protokoll

[4] A Report to the Secretary of Defense and the Director of Central Intelligence (February 28, 1994 Joint Security Commission) Washington, D.C. 20505

[5] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919)

[6] Négyesi Imre: Az önkormányzatok informatikai stratégiája és a Magyar Információs Társadalom Stratégia összefüggései (Hadtudományi szemle on-line, II. évfolyam (2009) 2. szám, 85-92. oldal HU ISSN 2060-0437)

Pölcz Péter – Pándi Erik – Pándi Balázs
ppolcz@codel.hu – pandi.erik@zmne.hu – balazs.pandi@gw.com

AZ INFORMÁCIÓVÉDELEM IDŐTÁLLÓSÁGA A KRITIKUS INFRASTRUKTÚRÁKBAN[1]

Absztrakt

Jelen közlemény az időtállóság kérdéskörét vizsgálja.

This publication studies the durability of information security procedures.

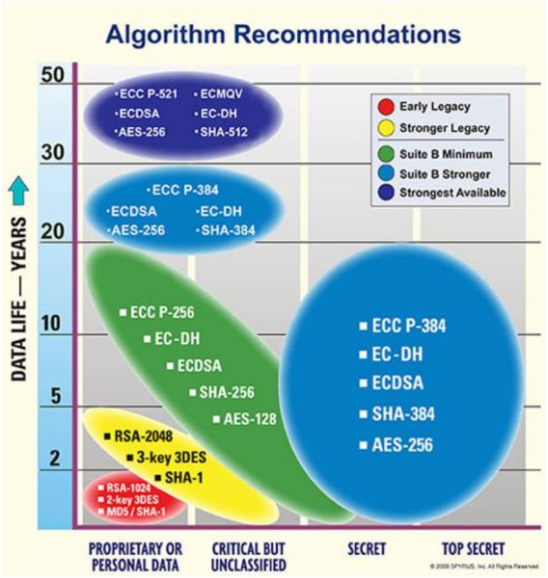
Kulcsszavak: *információbiztonság, rejtjelzés ~ IT security, cryptography*

BEVEZETÉS

A biztonságos információtárolás jelenlegi lehetőségei az adatok felhasználótól és rendszerektől való elzárásában valósul meg. Ennek oka, hogy a számítástechnikai kapacitás robbanásszerűen fejlődött a már lekódolt és kódolással tárolt adatok visszafejtésének idejét a Moore törvény szerinti növekedésből adódóan másfél évente felére csökkenti (csökkentheti), így rövid számítások szerint a jelenlegi 50 év-re titkosított adatok 2048 bites dekódolása várhatóan 10-15 éven belül lehetségessé válik.

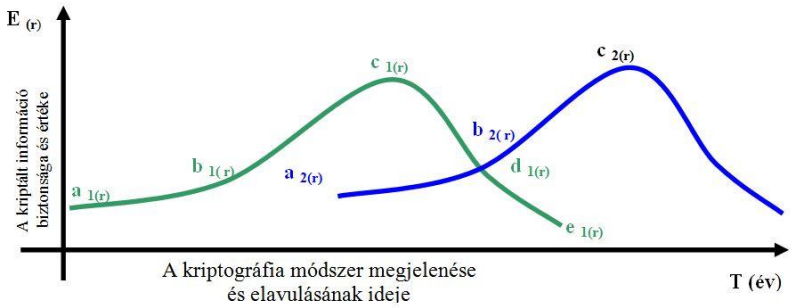
Azon törvények és szabályok melyeket korábban 10-20 éve megfogalmaztak, a személyi védelem viszonylagos időtállóságát leszámítva ma már erősen kétségbe vonhatók. Tudomásul kell vennünk, hogy a jelenlegi információvédelmi és rejtjelző világunk forradalmi, gyökeres változások előtt áll. A hagyományos technológiákat még használjuk és próbáljuk használhatóságukat időben kitolni, azonban viharosan gyors átalakulásra kell közben műszakilag és szakértelemben is felkészülni. Az eddig használt algoritmusok védelmi szintjét (minősített adatok voltát) és az algoritmusok időtállóságát mutatja a be a következő ábra:

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült



1. ábra

Fenti grafikonban foglaltak, a múltat és a jelen tükrözik, de időtállósága és biztonsága és védelmi szintjeik már erősen kétségbe vonható. A jövő kriptográfiája valahol a kvantum fizika és Einsteini relativitás határán fog tartózkodni, és tartóssága ismét a technológia fejlődése szerint először rövidebb majd hosszabb ideig lesz jellemző. Az információk és a kriptográfiai megoldások időtállóságát a következő diagrammal lehet szemléltetni:



2. ábra

Az „$a_{1(r)}$” pontban megjelenő új kriptográfiai technikák eszközeinek és algoritmusainak kiforrottsága, finomsága még csak bevezetési szakaszban van, ezért a védelem szintjét csak az elterjedtség alacsony volta adja. A „$b_{1(r)}$” a technológiák elterjedtsége már kialakult, ebben a fázisban a kódoló algoritmusok finomságának és hangolásának folyamata kezdődik, és ezzel megjelenik a védelmi szintek kiugrásszerű növekedése. A „$c_{1(r)}$” szakasznál a kiforrott algoritmusokkal történik a kódolás, de ezen fázisban már a látható határok miatt elindul az új technológia utáni kutatás. A „$d_{1(r)}$” szakaszban a technológia megbízhatósága és időtállósága erősen devalválódik, az új technológiák megjelenésével a rendszer kivezetésre kerül. Az „$e_{1(r)}$” fázisban a rendszer használata teljesen megszűnik, az alkalmazás és a hozzá tartozó technológia kivezetésre kerül, míg a kettes számú (kék) fejlesztések feljutnak és csúcsra jutnak.

1. JELENLEGI HATÁROK

A kriptográfia és adatvédelem jelenlegi határai a józan ész szerint 2048 bit-s AES titkosítás tájékán kell keresni. Lehetséges és valószínű, hogy az ábrán vázoltak szerint már a „c $_{1(r)}$ „ ponton a technológia már továbbjutott, tehát most kell nagyon a figyelni, és ha lehetséges az induló új módszereket átvenni, és új algoritmusokat kidolgozni. Nem szabad elfeledkeznünk a nemzeti megoldásokhoz való K+F feladatok sürgős elindításáról, és a környezetünk képességeinek (kódtörés) folyamatos elemzéséről. Jelenlegi határaink és képességeink bemutatása ezen közlemény jellegénél fogva nem lehetséges, de a mindenképen igyekszünk fontos üzenetként megfogalmazni és tárgyilagosan felbecsültetni.

2. HOVÁ TARTUNK? CÉLOK

A mennyiségi változás által kikényszerített minőségi változás a kriptográfia területén mindenképpen egy megújult rejtjelző rendszerek és védelmi rendszerek megjelenésében fedezhetők fel. Tehát jönnek az új technikák és technológiák, ennek legnagyobb esélyese a kvantum kriptográfia, amelyet már több ország is kutat és elemez.

A kvantummechanikai kriptográfia, Bennett és Brassard találmányát, az elemi részecskék különös viselkedési módjait használja adatvédelemre, vagyis az egyes fotonok (fényrészecskék vagy elemi hullámok) mérése szükségszerűen megváltoztatja azok állapotát, így az egymással kommunikáló felek között elhelyezett lehallgató berendezés nagyon hamar lelepleződik.

Az egymással "mágikus" kapcsolatban maradó, egyszerre keltett elemi részecske párok is felhasználhatók kvantum-számításokhoz, ezek nagy távolságból is azonnal észlelik a másik állapotának megváltozását, mindmáig megoldatlan problémát okozva az elméleti fizikusoknak.

Érdekes megfigyelés, hogy a kvantum-titkosítású adatátvitelben a biztonságos kulcscserét egy egyszeri alkalommal használatos kulcsú rejtjellel szokták megoldani. A titkosítás elméletének fejlődése tehát voltaképpen egy nagy kört futott be az évtizedek alatt, magasabb műszaki színvonalon visszatérve az első világháborúban felfedezett eredeti, feltörhetetlen kódoláshoz. Azt, hogy a kör a gyakorlatban is bezárul-e, még nem lehet tudni. A kvantum-kriptográfia alkalmazásához a számítógépeket külön optikai hálózati eszközökkel kell kiegészíteni, amelyek legalább 100 ezer dollárba kerülnek. Minden résztvevő páros közé direkt üvegszál kapcsolatot kell kihúzni és cserében szerény, egy otthoni ADSL vonal kapacitásának negyedét kitevő sebességet kapunk, legfeljebb százmérföldes távolságon. A módszert ezért ma csak a hagyományos titkosítás kulcscsere lépése helyett használják, ahol kicsi az adatátviteli igény.

Korunk eddig emlegetett „betegsége” és áldása a világháló másként az internet. Az internet elterjedésével közvetített és tárolt információink védelme is különleges hangsúlyt kell, hogy kapjon. Ezért készítenek és ír elő maga a törvény is a védendő rendszerekre vonatkozó katasztrófatervet. A katasztrófatervek szerepe az egyes rendszerek vagy adatok sérülésének, valamint védelmének folyamatos felügyelete és probléma esetén a programozott beavatkozás lehetősége. A katasztrófatervek mellett a másik megkerülhetetlen az informatikai biztonsági szabályzat, mely másik oldalról tárgyalja a védendő rendszerek hozzáférési és behatolási ellenintézkedéseinek összességét.

Mivel az események és rendszerkockázatok többségét ma már nem a technológiákban, hanem magában a felhasználó emberben kell keresni ezért fontos szem előtt tartani Heisenberg megállapítását, amely a következő:

„A kutatás tárgya többé nem a természet mint olyan, hanem az emberi kérdésfeltevésnek kitett természet”

3. NAPJAINK MAGYAR INFOSEC KIALAKÍTÁSÁNAK EGY LEHETSÉGES VÁLTOZATA

Napjaink magyar lehetőségeit alapul véve jelen fejezetben bemutatunk egy lehetséges rendszerkialakítást, amely a kriptográfiai elemeket, feldolgozó elemeket és a közvetítő elemeket is tartalmaz. A kialakítás Thales datacryptor IP rejtjelző eszközt, tempest számítógépet, valamint az iparban és biztonságtechnikában elérhető biztonsági elemeket tartalmaz.

3.1. Az eszköz rendeltetése:

Az IP rejtjelző eszköz a biztonságos és védett kommunikációt teszi lehetővé. Ennek elérésére a felhasznált algoritmus szerint 64-2048 bit mélységű titkosítást használ. Működése IP alapú hálózatokon keresztül történhet általában 100-1000 Mbps sebességgel (de vannak rendszerek amelyeknél már 5-10 Gbps sebességgel zajló átvitelről beszélhetünk). Az rejtjelzett adatátvitel számára közömbös, hogy az adatok számítógépes információk, vagy IP alapú telefonbeszélgetések, vagy videokonferenciák, esetleg rendszervezérlés, adat le- és feltöltés (megfelelő sávszélességek és módok megválasztása esetében).

3.2. A működtetéshez és elhelyezéshez szükséges tényezők

A rejtjelző eszköz elhelyezéséhez a következő információkat és adatokat kell figyelembe venni:

- a tápellátás: 110-230V, 50-60 Hz váltóáram;
- a rejtjelző eszköz felvett teljesítménye kisebb, mint 60VA;
- a rejtjelző eszköz a rátöltött algoritmusok és kulcsok nélkül, mint csupasz hardware nem képez adatvédelmi kockázatot;
- a rejtjelző eszköz elhelyezésére a környezet (telephely) elhelyezkedése és védelme alapján EUR 3-4 vagy BOVAS páncélszekrényben javasolt. Javasolt, hogy a páncélszekrény belső zárható fiókkal rendelkezzen, melyben az eszköz és a médiakonverter kerül elhelyezésre;
- a rejtjelző eszközt befoglaló páncélszekrény az előző pontban leírtak mellet megfelelő zárszerkezettel kell, hogy ellátott legyen. (javasolt a mechanikus tárcsás kombinációs zár);
- mivel a rendszer önvédő, a jelen leírásban később szereplő elektronikával kiegészítve így az önvédelmi funkciói azonnal reagálnak, ezért magára a páncélra a megfelelő minőség és zár mellett nem szükséges nyitási időzítés.(Ez lehetővé teszi, hogy a megfelelő jogosultsággal rendelkező személy rövid időn belül az eszközt használja, és azon forgalmazzon. Tehát nem szükséges a nyitási késleltetést kivárni, és ezzel esetleg az információ elévülését kockáztatni);
- a rendszerterv kialakításakor, figyelembe vettük, hogy magát a berendezést és védelmi rendszerét autonóm módon magára lehet hagyni, oly módon hogy az behatoláskor, illetéktelen hozzáférési kísérletekor, külső áramforrás megszüntetésekor önállóan és visszaállíthatatlanul törli a kulcsokat és rejtjelző algoritmusokat;
- a rendszer összeállításakor javasoljuk (de nem feltétlen szükséges, mivel a kommunikáció a rejtjelző és a számítógép között optikai kábelen megy, így az lehallgathatatlan), hogy az adatforrásként szereplő számítógépeket (lehetőleg Tempest minősítésűeket) ugyanazon páncélszekrényben kerüljenek elhelyezésre, mint a rejtjelző eszköz. (lásd javasolt összeállítás).

3.3. Az eszköz minősítése

A rejtjelző eszköz jelen algoritmussal és kulcsokkal (Triple DES és Rijndael AES), max 2048 bit kulcsmélységgel alkalmas a BIZALMAS információk védett küldésére, fogadására, illetve védett / rejtjelzett beszéd és videó csatorna kiépítésére. A rendszer hardverének módosítása nélkül a berendezés alkalmassá tehető nemzeti minősített anyagok forgalmazására, az eszközt működtető szoftver (algoritmus) és kulcs cseréjével.

3.4. A rejtjelző eszköz önvédelmi funkciói

A jelen rejtjelző eszköz logikai védelmét autonóm belső és fizikai külső részre oszthatjuk. Autonóm funkciók:

- a beállított szabályok szerint KEK, DEC kódok önálló cseréje, mely lehetővé teszik, hogy a kulcscserék automatikusan lezajlódjanak, és így a nyílt vonalon lévő adatok beavatatlannak keveredjenek;
- a hardverre csak feltölteni lehet a kódot és algoritmust, letölteni nem lehetséges, így az illetéktelen kezekbe kerülés esetén sem kell új algoritmust készíteni;
- a beépített önvédelmi funkcióknak megfelelően a mesterkulcs (fizikai kulcs) beállítása szerint a rejtjelző eszköz törli minden tartalmát, ha megmozdítják, illetve az operátora azonnali gombnyomással törlést kezdeményez;
- a rendszer rugalmasan kezelhető, és központilag a védett csatornán keresztül ellenőrizhető, illetve menedzselhető;
- kiegészítő elektronikával, külső behatolás védelmi rendszerrel (elektronikus biztonsági rendszer) összekötve behatolás, illetéktelen belépés esetén önműködően kulcs- és algoritmustörlés.

A fizikai funkciók:

- az eszköz a fizikai kulcs beállításától függően, kerülhet önvédelmi, szállítási és törlési állapotba;
- az önvédelmi állapot esetén a rendszer törli minden tartalmát, ha megmozdítják, vagy a törlési gombját megnyomják (még áramtalanított esetben is);
- a törlési állapotba kapcsolás esetén a törlési gomb megnyomásával azonnali kulcs és algoritmustörlést hajt végre a rendszer (még áramtalanított esetben is);
- a szállítási (tansport) állapotba a rendszer önvédelme deaktiválásra kerül. Ilyen állapotba célszerű kulcs és algoritmus feltöltése nélkül szállítani;
- az eszköz felnyitás ellen védett. Kinyitás és ennek kísérlete esetén a rendszer mind kikapcsolt (áramtalan esetben is) törli és megsemmisíti belső fizikai tartalmát.

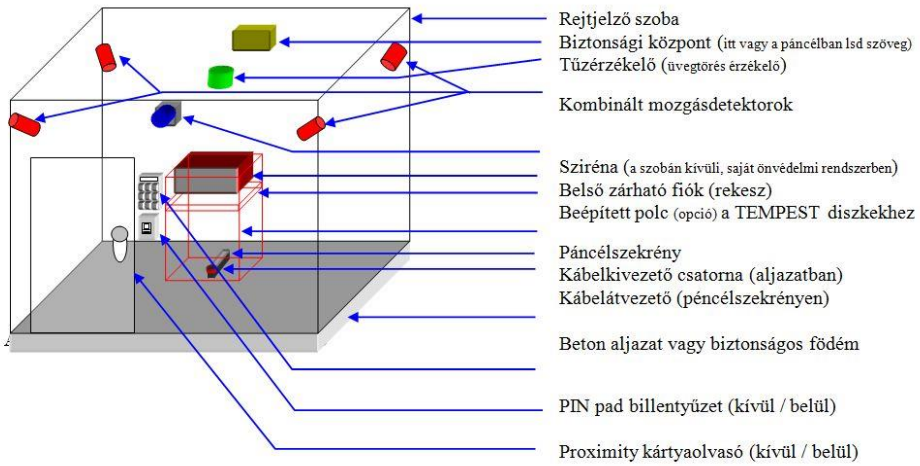
Az eszköz alkalmas arra, hogy minimális helyszíni felügyelettel a menedzselő központból új algoritmus és kulcsokat töltsön le és kezdjen használni. Az eszköz a fizikai kinyitási kísérletre helyreállíthatatlan állapotba kerül (önmegsemmisítés), így csak cserével javítható.

3.5. A rejtjelző eszköz környezeti kialakítása

A rejtjelző eszközt magába foglaló páncélszekrénnyel és szobával szemben támasztott követelmények kialakításánál figyelembe veendő tények:

- a szobának és az ajtajának kialakításakor legalább 20 perces ellenállási képességgel kell rendelkeznie;

- a páncélszekrénynek legalább 20 perces behatolási ellenálló képességet kell tudnia biztosítani;
- az alkalmazott mozgásérzékelő rendszer detektorainak kombinált (infra és radar) típusúaknak kell lennie;
- az üvegtörés érzékelőt ugyanazon védelmi rendszerbe kell bekötni mint a mozgásérzékelőket;
- A füst és tűzdetektorokat (az épület központi védelmén kívülieket) szintén a szoba védelmi rendszerének központjába kell bekötni;
- az ajtóknak nyitásérzékelővel kell rendelkeznie, melynek a szobán belül és befúrt típusnak kell lenni és a szoba védelmi elektronikai központjába kell bekötni;
- az ajtónak a külső és belső nyitását proximity kártya és a hozzá tartózó PIN kód megadásával a központi védelmi rendszer végzi (mágneszáras megoldással, javasoltak a síkmágneses zárak). Belülre lehetséges a vésznyitó gomb felszerelése;
- az ajtó nem rendelkezhet kilinccsel, nyitását és zárását csak az elektronika végezheti;
- a szoba ajtajára mechanikus behúzó rendszert kell szerelni;
- amennyiben a szoba ablakkal is rendelkezik, úgy az ablakokat is saját nyitásérzékelővel kell ellátni;
- a szoba belátásvédelmét függönnyel meg kell oldani;
- a rejtjelző eszközt (és a javasolt TEMPEST számítógép adathordozójának) tárolását végző páncélszekrény védelmét a mechanikus, kombinációs forgótárcsás számzárral kell ellátni;
- a páncélszekrényre nyitására időzítőt nem javaslunk;
- a páncélszekrénynek rendelkeznie kell egy belső zárható fiókkal, amelynek mérete 22 cm x 50 cm x 46 cm.



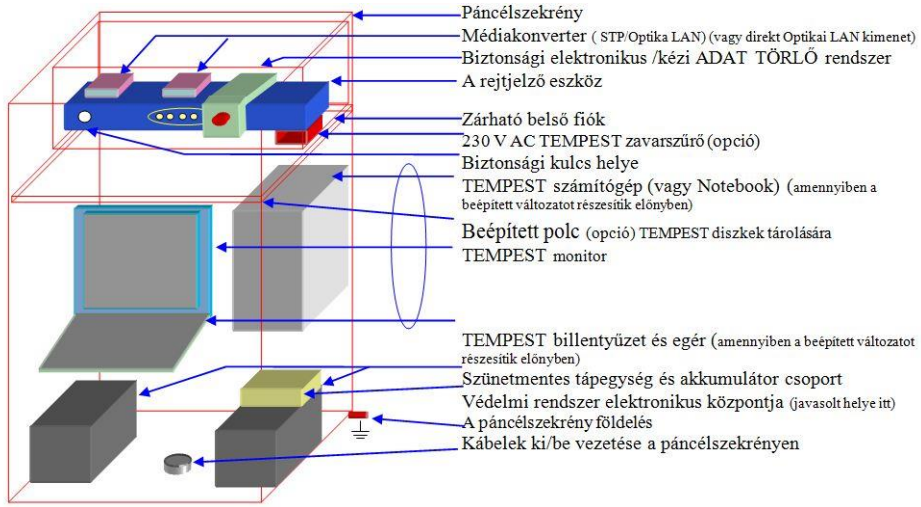
3. ábra

A páncélszekrény belső kialakításánál a következőket vettük figyelembe:

- a páncélszekrénynek az önvédelmi funkciók miatt nem szükséges extrém erős kivitelűnek lennie;
- a belső elrendezésnél a belső zárható fiók esetében a rendszer alkalmas a rejtjelző eszköz TEMPEST követelményeinek kialakítására;

- a kommunikációs, rejtjelző rendszer be- és kimenete optikai kábelen keresztül történik a lehallgathatóság kivédésére;
- a rejtjel eszköz fiókjára célszerű felszerelni egy 230V-os hálózati kapcsolót mellyel a fiók kinyitása nélkül a hálózat kikapcsolhat;
- a rendszerrel lehetséges dolgozni zárt és nyitott nagyajtó esetében (mivel a kompromittáló kisugárzást jelentő eszközök a bezárt fiókban vannak.);
- a rendszer alkalmas arra, hogy a TEMPEST számítógépet, vagy notebokot is befogadja;
- a kialakításból adódóan, amennyiben TEMPEST számítógépet használunk, úgy lehetőség van (mindkét optikai szál –be és kimenet- kivezetésére) a teljesen zárt szekrény használatára;
- a szekrényben elhelyezett polc lehetővé teszi, hogy külső TEMPEST minősítésű számítógép adathordozóját a szekrényen belül elhelyezzük. (Figyelem: a szekrény önvédelmi rendszere csak a titkosítót és a hozzá tartozó sw-t védi, illetve illetéktelen hozzáférés esetén törli. Tehát az elhelyezett adathordozón lévő adatoknak rejtjelzetteknek kell lenniük és a hozzá tartozó kulcsok, és kártyát máshol kell tárolni);
- az önvédelmi rendszer központja saját akkumulátorral van ellátva így a rejtjelző eszköz védelmét ellátó akkumulátor csoporttól független rendszert alkot;
- az akkumulátor csoport lehetővé teszi, hogy áramkimaradásos veszély esetén személyes beavatkozással a hálózatra mégy üzenetet lehessen küldeni.

A javasolt kialakítás:



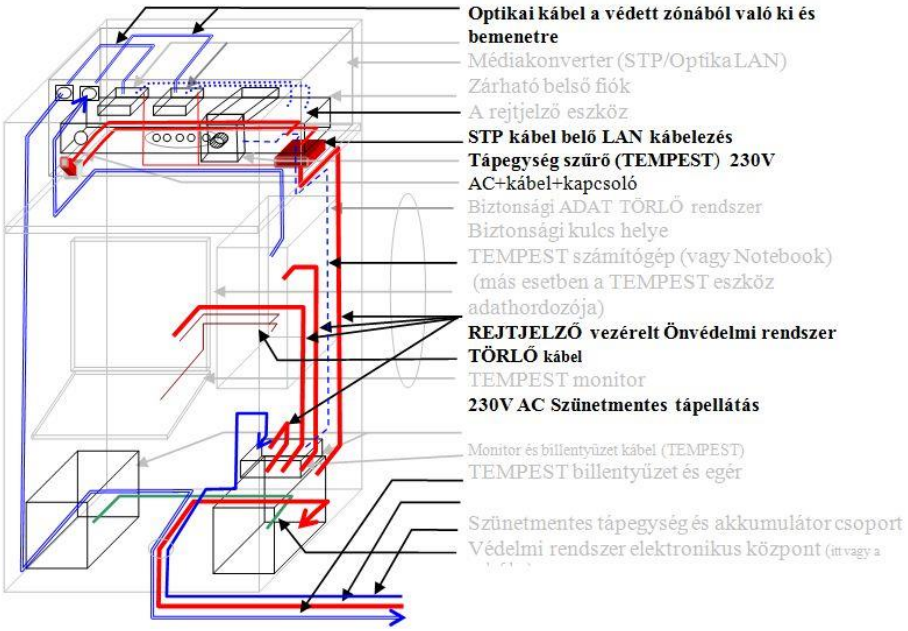
4. ábra

A páncélszekrény belső kábelezése a következők szerint oldható meg:

A páncélszekrény és az abban elhelyezett eszközök védelmét maga a szekrény, a benne és a környezetében elhelyezett elektronikai rendszerek és érzékelők közösen látják el. A páncélszekrényen belüli kábelezés nem kíván extra megoldásokat. Az egyetlen kiemelt védelmi pont a belső fiókban lévő rejtjelkészülék és média konverter melynek tápellátására TEMPEST tápszűrő alkalmazását javasoljuk.

A kimenő adatvédelmet az optikai kábel megoldás biztosítja. A rendszer működőképességének és áthidalási időinek biztosítására használjuk a belső szünetmentes energiaforrást. A kivezető kábelek a páncélszekrény alján kialakított átvezető csatornán

mehetnek. A biztonsági és vagyonvédelmi rendszer tápellátása a központból történik, mivel ez saját akkumulátorcsomaggal van ellátva a folyamatos működés és a szabotázsvédelem biztosítása miatt.



5. ábra

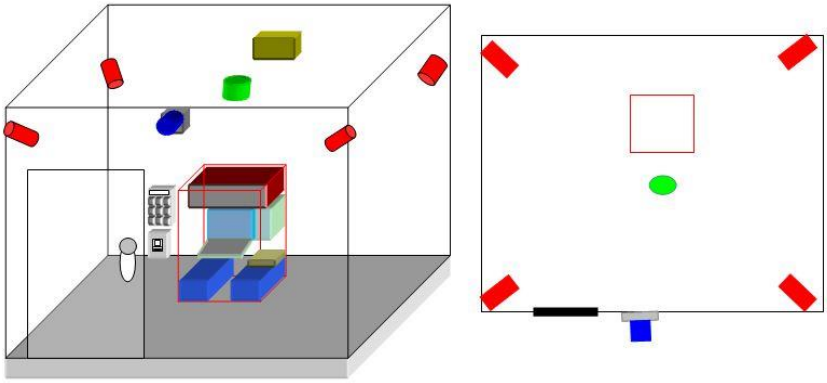
3.6. A rejtjelző eszköz kulcsbeállításai és biztonsági funkciók

A rejtjelző eszköz helyes kulcskezelése elengedhetetlen feltétele a rendszer és önvédelmi funkciók szabályos működtetéséhez. A rejtjelző eszköz kiegészítésre kerül egy külső védelmi elektronikával, amely a szoba elektronikus védelmi rendszerével van összeköttetésben, illetve a külső védelmi rendszer jelzésére a eszközön a kulcs- és algoritmustörléshez szükséges gombot az elektronika megnyomja. Ugyanezen blokkon foglal helyet az azonnali kézi kulcs és algoritmus törlés gomb. A rejtjelző eszközön lévő kulcs mindig egyedi és géphez kötött.

3.7. Az eszköz elhelyezése a szobában

Nem javasoljuk a páncélszekrényt közvetlenül a fal mellé elhelyezni, ha a fal túloldalán lévő helyiség növeli a kockázatot, például:

- a fal nem tömör és nem beton;
- a szomszédban nem saját terület található.



6. ábra

A szobába való belépést a minősítés szintjének megfelelően lehet, illetve kell módosítani (ezen ajánlást és előírást a szakhatóság javaslatára kell elvégezi), javasolt a biometrikus azonosítás, pl. újlenyomat, írisz vagy tenyér érhálózati azonosítás.

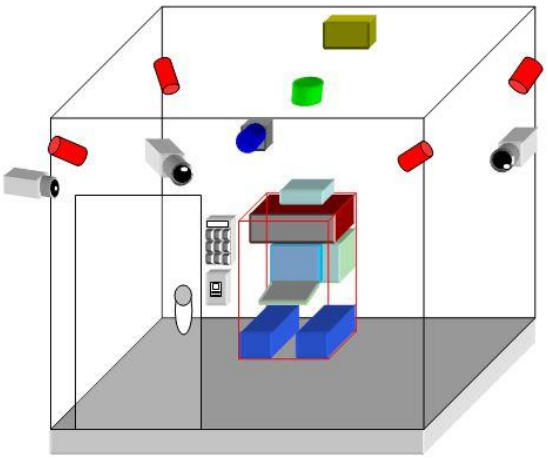
A védelmi rendszer élesítése csak a szobán belülről, míg deaktiválása csak a szobán kívülről (belépés előtt) lehetséges. Ezen eljárással megakadályozható, a „véletlen" belépés riasztása és az elektronikai rendszer szükségtelen beavatkozása (kulcs, és algoritmus törlés). Az esetlegesen „mégis" bekövetkező jogosult belépés esetén a beriasztott és védett területre az illetőnek lehetősége van az elektronikus rendszer késleltetése idején a kulcs és kód ismételt megadására a beléptetési ponton.

A páncélszekrényen belüli önvédelmi rendszer ÉS kapcsolatban van a riasztó, és elektronikus és/vagy személyi védelmi rendszerrel, olyan módon, hogy amennyiben a területre történő illetéktelen behatolás történt ÉS az engedélyezett időn belül nem történik személyi vagy védelmi válaszlépés, akkor a védelmi elektronika parancsot ad a rejtjelző eszköz kiegészítő áramkörének a kulcs és algoritmus azonnali törlésére. A mozgásdetektorok, falfúrás érzékelő detektorok, üvegtörés érzékelő detektorok jelzése valamint a páncélszekrény mozdítás érzékelőjének együttes hatására a rendszer azonnali kód- és kulcstörlést kezdeményez.

Javasolt, a védelmi rendszer önálló figyelmeztető SMS küldése mellett, a riasztás tényének jelzése az épület biztonsági szolgálata, valamint a helyszínen tartózkodó saját erők számára, illetve lehetőség esetén akár a védett csatornán történő üzenetküldésre az eseményről.

3.8. A rendszert kiegészítő lehetőségek

A rendszer kiegészíthető belső kamera rendszerrel és védett digitális videó rögzítővel vagy központtal, melyet úgy kell elhelyezni, hogy a tevékenységet nem, de a védett zónába való belépést, illetve mozgást rögzítse, illetve közvetítse azon időben mikor rejtjeltevékenység nem folyik.



7. ábra

Célszerű a rendszert saját tűzoltó védelmi rendszerrel ellátni, illetve ha az illetékes hivatal nem érzi ezt szükségesnek, akkor a tűzvédelmi rendszert a szoba saját védelmi rendszerébe bekötni.

Amennyiben a védett információ és rendszer megköveteli a hosszabb áramszünet esetére (vagy áramszünetnek álcázott akkumulátor lemerítéses támadás esetére) célszerű a védelmi rendszer saját aggregátorral történő tartalék áramforrásának biztosítása.

A szoba védelmi és észlelő rendszerét nem szabad összekötni más idegen védelmi rendszerekkel. A szobának csak a riasztó rendszerét szabad, illetve célszerű bekötni az idegen védelmi rendszerbe, de oda is csak kijelzéses, riasztásos módban.

Magasabb védelmi szintek estén alkalmazható még passzív padozatra helyezett járásérzékelők valamint, infra- és, vagy lézersorompók kialakítása melyek szintén a saját szoba elektronikus központjába kerülnek bekötésre.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az IP alapú rejtjelző eszközök a felhasználhatóságuk sokoldalúságából adódóan, nagyon szenzitív eszközök, melyek környezeti és önvédelmi biztonsága illetve biztosítása ebből adódóan sokoldalú megfelelést és biztonságot követel. Napjaink és a jövő védett és biztonságos kommunikációját lehetővé tevő berendezések, és környezetük védelmét legalább olyan komolyan kell venni, mint a védendő információt.

Az információs rendszerek világában a legnagyobb érték maga a jó és pontos információ és adat. Az nyer, aki ezen adatokat mielőbb megszerzi és oly módon juttatja el a feldolgozókhoz és felhasználókhoz, hogy annak tartalma a védettségéből kifolyólag mások számára rejtve és a biztonságosan jusson át egy információéhes és nagyon kíváncsi hálózaton.

Összességében azon eredetei igazságra hívnánk fel a figyelmet, hogy aki elveszti vagy felelőtlenül kezeli személyes adatait és titkait az a fejlődés és az idő folyamán egyre rosszabb pozícióba kerül, mivel mindig van valaki, aki ezt az információt fel akarja és fel is tudja használni.

FELHASZNÁLT IRODALOM

[1] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal)

[2] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919)

[3] Andrew S. Tanenbaum: Számítógép hálózatok 97-101. oldal.

[4] Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője (MK KBH Szakmai Szemle 2009. 3. szám, 35-50. oldal, ISSN 1785-1181)

[5] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05.-06.)

Kerti András – Pándi Erik – Töreki Ákos
kerti.andras@zmne.hu – pandi.erik@zmne.hu – toreki.akos@zmne.hu

A VEZETÉSI ÉS INFORMÁCIÓS RENDSZER BIZTONSÁGA[1]

Absztrakt

Jelen közlemény a vezetési és információs rendszer egyes biztonsági kérdéseit dolgozza fel.

This publication deals with some of the questions related to the security of the Command and Information System.

Kulcsszavak: *információvédelem, VIRTAR ~ information security, VIRTAR*

BEVEZETÉS

A kormányzati és üzleti szervezetek nagymértékben az információk használatára támaszkodnak üzleti tevékenységük irányítása során. Az információ és a szolgáltatások bizalmasságának, sértetlenségének, rendelkezésre állásának, letagadhatatlanságának, számonkérhetőségének, azonosíthatóságának és megbízhatóságának elvesztése igen káros hatással van a szervezet üzleti működésére. Következésképp az információk védelme és az informatikai rendszerek biztonságának menedzselése a szervezeten belül kritikus fontosságú [1]. Az MSZ 13335-es szabványból citált idézet sehol sem olyan aktuális, mint a honvédségi rendszerekben, ahol adott esetben (konfliktusok, missziók) emberéletek és akár a küldetés sikere is múlhat az információbiztonságon.

1. AZ INFORMÁCIÓBIZTONSÁG SZAKTERÜLETEI

Az információbiztonsági feladatok szakterületekre bontásához többfajta modell létezik, amelyek közül a vizsgálatunkhoz a NATO modellt választottuk. Az információbiztonság NATO modelljét a „C-M(2002)49 Security Within The North Atlantic Treaty Organisation (NATO)” című dokumentum foglalja magába, amely a NATO-n belül a minősített információk védelmének alapdokumentuma. A NATO az információbiztonság feladatait négy fő kategóriába osztja:

- fizikai biztonság;
- személyi biztonság;
- dokumentum biztonság;
- elektronikus információbiztonság.

Az elektronikus információbiztonság feladatai további öt feladatcsoportba oszthatók, úgymint:

- számítógép és helyi hálózat (LAN) biztonság;
- hálózatok biztonságos összekapcsolása;
- rejtjelbiztonság;

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

- elektromágneses kisugárzás biztonság vagy másképpen kompromittáló kisugárzás biztonság;
- átvitelbiztonság.

A biztonsági részterületek között fontossági sorrendet, alá-fölérendeltségi viszonyt nem lehet meghatározni.

2. AZ INFORMÁCIÓBIZTONSÁGI SZAKTERÜLETEK ALAPVETŐ FELADATAI

A szakterületek nem szeparálhatók el egymástól, néhol bizonyos átfedések lehetségesek. Az elektronikus információbiztonság két legrégebbi szakterülete a rejtjelbiztonság és az átvitelbiztonság (régi szakterminológiával élve híradóbiztonság) amelyeknek akkor van szerepük, ha az információ az ellenőrzött területen kívülre kerül. Mind a rejtjelbiztonság kérdéseivel, mind a többi három biztonsági területtel (számítógép és helyi hálózat [LAN] biztonság, a hálózatok biztonságos összekapcsolása, elektromágneses kisugárzás biztonság) a szakirodalom egyre bővülő tárháza foglalkozik, azonban az átvitelbiztonság kérdésköre nagyrészt feldolgozatlan.

3. ÁTVITELBIZTONSÁG

A szakterület feldolgozatlansága alapvetően két okra vezethető vissza:

- a katonai hálózatokban az átviteli rendszerek nem csak homogén számítógépes hálózatokból állnak, mint a mai polgári architektúrák, hanem tartalmaznak a katonai innfokommunikációs hálózatokra jellemző eszközöket is (pl.: különféle rádiók), egyúttal minden rendszerelem különböző fenyegetettségekkel is szembenéz, ezért nehézkes az egységes védelmi profil kidolgozása;
- a polgári életben a legtöbb szereplő az átviteli utat megvásárolja egy szolgáltatótól (pl.: Internet kapcsolat, mobiltelefonos szolgáltatás), így e rendszerek biztonságát a szolgáltatónak kell megoldania. A gyakorlat ugyanakkor azt mutatja, hogy behatárolt azon szolgáltatóknak a száma, amelyek e kérdéskörrel foglalkozni tudnak. A békeidőszakokban a katonai rendszerekben is ilyen jellegű megoldások dominálnak, azonban fel kell készülnünk olyan helyzetekre is amikor polgári cégek szolgáltatásait, vagy előre telepített zártcélú hálózatokat nem tudunk igénybe venni.

3.1. Az átviteli út és az átvitelbiztonság meghatározása

Az átvitelbiztonság feladatainak tisztázásához meg kell határozni az átviteli út és az átvitelbiztonság fogalmát. Első megközelítésben az átviteli út a transzporthálózatot megvalósító eszközök összessége. Amennyiben feltételezzük, hogy az ellenség minden olyan összeköttetésünket értékelni és manipulálni tudja, amelyet nem tartunk folyamatosan a felügyeletünk alatt akkor azt az összeköttetést is ide kell sorolni, ami ugyan a belső hálózat kapcsolatait valósítják meg, de az általunk ellenőrzött teret elhagyják, illetőleg elhagyhatják. Ennek tükrében az átviteli út fogalma nem más, mint: *Mindazon hír, adat és információ továbbító csatornák (továbbiakban összeköttetések), jellegüktől és felépítésüktől, összetételüktől és hosszúságuktól függetlenül, amelyek a szerepüket úgy töltik be, hogy közben az általunk ellenőrzött területet határain kívülre kerülnek vagy kerülhetnek.*

Adaptálva az információbiztonság elveit, az átviteli út biztonság, vagy másképpen az átvitel biztonság alapvető feladata: *Az információk rendelkezésre állásának, sértetlenségének, és bizalmasságának megőrzése az átviteli út folyamán, valamint az átviteli utat megvalósító eszközök rendelkezésre állásának, sértetlenségének biztosítása.*

3.2. Az átvitelbiztonság feladatainak és folyamatainak meghatározása

Véleményünk szerint egyrészről az átvitelbiztonság feladatainak és folyamatainak meghatározáshoz a kockázatkezelés végrehajtása a legjobb módszer. Másrészről a biztonsági ellenintézkedések minden esetben valamiféle gátak az információáramlás útjában, másrészt erőforrásokat emésztenek fel, éppen ezért a biztonsági ellenintézkedéseket gondosan, minden esetben az adott helyzetnek megfelelően, költséghatékonyan kell kivitelezni. Ennek végrehajtásához célszerű elkészíteni a vezetési és információs rendszer technikai alrendszerének (VIRTAR) kockázatelemzését és kockázat menedzsmentjét.

Az információs rendszerek kockázatkezelése az információbiztonság jelenleg egyik legjobban fejlődő részterülete, amely jelenleg nem mutat egységes képet a különböző szervezetek módszereiben. Az ISO és az IEC45 2008 júniusában kiadta a 27005-ös szabványát és ezzel egyrészt korszerűsítette a kockázatkezelés szemléletmódját, másrészt a 13335-ös szabványcsalád első négy tagját hatálytalanította. Ez a korszerűsítési folyamat még nem fejeződött be az összes információbiztonsággal foglalkozó szervezetnél. Erre jó példa lehet a 2008 júniusában megjelent Közigazgatási Informatikai Bizottság 25. számú ajánlása, amely még a 13335-ös szabványcsalád szerinti kockázatkezelést alkalmazza, valamint az ENISA, amely diplomatikusan nem tesz különbséget a különböző kockázatkezelési módszerek között, viszont a honlapján lehetőséget nyújt ezek összehasonlítására.

A Magyar Honvédség hivatalos információbiztonsági politikája e témakörben rögzíti, hogy a kockázatelemzést

- minősített adatokat kezelő rendszer, több szervezet által közösen használt vagy üzemeltetett rendszer, MH-szintű rendszer esetében kötelezően;
- egyéb adatkezelő rendszerek esetében a NATO, EU, nemzeti elektronikus adatkezelésre feljogosított rendszerek felügyeletét ellátó hatóság, illetve az információvédelem szakmai felügyeletét ellátó honvédelmi szerv döntése szerint kell végrehajtani [2].

Fentiek alapján a kockázatkezelési folyamatot az átviteli utak tekintetében végre kell hajtani, mivel kezelt adatok minősítési szintjétől függetlenül az átviteli utakat több szervezet használja (elöljáró-alárendelt). A kockázatkezelés azonban csak akkor lehet eredményes, ha ez nem egyszeri, hanem periodikus folyamat. Ezért a kockázatelemzés eredményeit időről időre felül kell vizsgálni és ha új kockázati tényező megjelenését tapasztaljuk újra kell tervezni az ellenintézkedéseket, illetve az egész kockázatkezelési folyamatot az új adatokkal meg kell ismételni.

Szintén az eredményességet javíthatja, ha a kockázatokkal kapcsolatos információkat megosztjuk a kockázatkezelést végző szervezetekkel, illetőleg ezeket a megosztott információkat felhasználjuk a kockázat menedzsmentben. A szabvány által bemutatott folyamat azonban olyan, mintha a végrehajtott folyamat egyszeri cselekvés lenne, azonban a kockázatkezelés (vagy kockázatmenedzsment) nem egy egyszeri cselekmény, hanem egy folyamat, amelyet az információ feldolgozó rendszer és így az átviteli teljes életciklusa alatt folyamatosan végre kell hajtani.

Véleményünk szerint az átvitelbiztonsági kockázatok értékelésekor, vagyis az átvitelbiztonság meghatározásához a legfontosabb feladat a hatókör meghatározása. Az ISO/IEC 27005 szabvány megítélésünk szerint erre nem ad elegendő fogódzót, ezért célszerűnek tartjuk a két szabvány munkafolyamatainak kombinációját alkalmazni.

A kockázatfelmérés folyamatában a különböző folyamatok még további cselekvésekre bonthatók. Annak érdekében, hogy a kockázatokat teljes mértékben azonosítani tudjuk a következő részfeladatokat kell végrehajtani:

- a vagyontárgyak azonosítása, amelyek közé a fizikai vagyontárgyakat, az információkat, a folyamatokat és a személyzetet sorolja a szabvány;
- fel kell mérni a valószínű fenyegetéseket, amelyek minden egyes esetben mások és mások lehetnek, de ha azonosak, akkor is hangsúlyuk különbözők;
- be kell azonosítani a már létező ellentevékenységeket és azonosítani kell a sebezhetőségeket, amelyeket a fenyegetések ki tudnak használni.

Amennyiben mindezeket a folyamatokat sikerült végrehajtanunk, akkor azonosítani tudjuk a kockázatok következményeit. A kockázatok becslésénél figyelembe kell venni és ki kell értékelni az azonosított következmények hatásait a vizsgált rendszerre, illetőleg figyelembe kell venni az azonosított és kiértékelt következmények előfordulásának valószínűségét. A két eredményből megkapjuk a kockázatok szintjét.

A kiértékelésekor a kockázatok szintjének figyelembevételével egy olyan sorba rendezett listát kapunk, amely megmutatja, hogy melyek azok a kockázatok, amiket el tudunk fogadni és melyek azok, amelyek ellen új ellenintézkedést kell bevezetnünk. Az ellenintézkedések megválasztása után meg kell vizsgálni, hogy a fennmaradó maradványkockázatok elérik-e az elfogadható szintet, avagy sem. Természetesen abban az esetben, amikor nem érik el ezt a szintet akkor új ellenintézkedéseket kell bevezetni.

3.3 A kockázatkezelés végrehajtása az átviteli út biztonsága tekintetében

Az átviteli út kockázatelemzése csak abban különbözik az egyéb kockázatelemzésektől, hogy más hangsúlyt kapnak a sebezhetőségek és fenyegetések. Ezen megállapítás kifejezetten igaz akkor, amennyiben egy missziós vagy egy harci feladatot hajt végre az adott katonai szervezet, ezért a továbbiakban erre az eshetőségre koncentrálva végezzük el a vizsgálatokat.

3.3.1. Az átvitelbiztonság hatókörének meghatározása

3.3.1.1 A szervezeti információbiztonság politika áttekintése

A jelenleg is érvényben levő MH információbiztonsági politika az átviteli út biztonságról a következőket fogalmazza meg: *„Az elektronikus adatkezelő rendszerekben alkalmazott átviteli eljárásokat és biztonsági mechanizmusokat a kezelt adatok bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó követelmények szerint kell kialakítani.”* [3]. Ebből az idézetből azonban nem derül ki, hogy melyek ezek a követelmények, illetőleg az sem, hogy a jogalkotó az átviteli útbiztonsággal, illetve az átviteli protokollokkal kívánt-e foglalkozni. Ezek alapján fontos kérdésként merül fel, hogy mi lehet az információbiztonság feladata az átviteli út vonatkozásában.

Első megközelítésben a C-M(2002)49-ből már citált idézet alapján első feladat az információk és a rendszer bizalmasságának, sértetlenségének, rendelkezésre állásának biztosítása. Véleményünk szerint bizonyos esetekben sokkal fontosabb, hogy a vezetés folytonosságát biztosítsuk.

Összefoglalva az információbiztonsági politika átviteli út biztonságával foglakozó részben le kell szögezni, hogy az információvédelmi rendszabályoknak az átviteli út során biztosítaniuk kell a vezetés folytonosságát, amennyiben szükséges a rejtett vezetést, miközben megőrzik az információk és a rendszer sértetlenségét, bizalmasságát, és rendelkezésre állását.

3.3.1.2 A hálózati architektúrák és alkalmazások áttekintése

Véleményünk szerint ahhoz, hogy a VIRTAR felépítését vizsgálni tudjuk célszerű áttekinteni a Magyar Honvédség által végrehajtott missziók információs kapcsolatait [4]. A missziót végrehajtó alakulatnak összeköttetésben kell lennie:

- az elöljáró szervezet törzsével, ahonnan gyakorlatilag a feladat végrehajtásához szükséges intézkedéseket, és egyéb információkat kapja;
- a hazai területen települt katonai vezető szervezettel, ami jelenleg a missziók esetében a Magyar Honvédség Műveleti Központ;
- azokkal az alárendelt csapatokkal, szervezetekkel, amelyek a feladataikat nem a szervezet települési helyén hajtják végre. Ilyenek lehetnek például a különböző járőrök, illetve az iraki misszió idején a konvoj kisérések.

Természetesen a szervezetnek kapcsolatot kell fenntartania a szomszédos egységekkel, alegységekkel, illetőleg a támogató szervezetekkel. Ezek lehetnek más nemzeti szervezetek, szövetséges csapatok és ebbe a kategóriába kell sorolnunk a nem katonai szervezeteket is, amelyek ugyanabban a misszióban tevékenykednek.

A misszió sikere érdekében a missziós csapatoknak el kell fogadtatni a misszió célját a helyi lakossággal, ezért mindenképpen összeköttetésben kell állniuk a helyi közigazgatási, illetve más civil szervezetekkel és helyi vezetőkkel [5].

Modern korunkban egy misszió sikere elképzelhetetlen a hazai közvélemény támogatása nélkül, ahhoz, hogy ezt a támogatást elnyerjük mindenképpen gondoskodnunk kell a misszióban szolgálatot teljesítő katonák hazai kapcsolattartási lehetőségeiről. Ez a feladat mind szervezési mind biztonsági szempontból nagy kockázatokat rejt, ezért fokozott gondossággal kell azt tervezni.

3.3.1.3 A hálózati kapcsolat típusainak azonosítása

A 13335-ös szabvány több kapcsolati típust felsorol, amelyek közül az átviteli út szempontjából figyelembe véve a kérdéskört az alábbi kapcsolati típusok lehetségesek [6]:

- Kapcsolódás egy szervezet földrajzilag elkülönülő részei között, pl.: a parancsnoki (helyi és nemzeti) kapcsolatok;
- A szervezet telephelyei közti kapcsolatok és a távmunkát végző személyek kapcsolódásai, pl.: az alárendeltekkel történő kapcsolattartás;
- Kapcsolódás más szervezetekkel, pl.: a helyi közigazgatási szervek, támogatók, együttműködőkkel történő kommunikációs csatornák;
- Kapcsolódás nyilvános környezetekkel pl.: a katonák kapcsolattartása a családjukkal.

3.3.1.4 A hálózati jellemzők, bizalmi kapcsolatok áttekintése

A VIRTAR-t elsősorban a hálózatok megvalósulása alapján célszerű csoportosítani. Ezek alapján kétféle hálózattípust lehet megkülönböztetni:

- a saját erőink által létesített hálózatok;
- szolgáltatótól bérelt hálózatok.

A szolgáltatótól bérelt hálózatokhoz soroljuk a szövetséges csapatok által számunkra rendelkezésre bocsátott hálózatokat is. Ezen hálózatoknak az átviteli út biztonság szempontjából problémája, hogy a biztonsági tulajdonságait nem tudjuk megváltoztatni, azokat csak megrendelni és értékelni tudjuk. Természetesen más biztonsági osztályba sorolhatjuk és másképpen értékelhetjük a hálózatokat, amennyiben egy NATO szövetséges vagy NATO által biztosított, másképpen, ha egy polgári szolgáltatótól bérelt hálózatról van szó. Az első esetben a NATO biztonságpolitikájában leírtak szerint csak annyit kell tudnunk, hogy az engedélyező és jóváhagyó hatóság megfelelőnek találata-e hálózatot, illetve a 3.3. alfejezetben említett kivételről van-e szó.

A második esetben a biztonsági értékelés nehezebb, de lehetséges. Tudnunk kell a szolgáltatóról hogyan kezeli a biztonságot, megfelel-e a különböző szabványoknak, netalán egy nemzetközi szabvány szerint auditált hálózatról van-e szó. Amennyiben lehetőségünk van választani a szolgáltatók közül azt a szolgáltatót kell választani, amelyik nagyobb garanciát nyújt az információbiztonság területén. A szolgáltatók és a szolgáltatások összehasonlításához szintén segítséget nyújthatnak a nemzetközi szabványok, mint például az MSZ ISO/IEC 15408 szabványcsalád.

A saját szakcsapataink által megvalósított átviteli utak felosztása a biztonsági kockázataik szerint követi a technikai megvalósítási struktúrát, amely alapján megkülönböztethetünk vezetékes és vezeték nélküli, illetve vegyes kivitelezésűeket [7]. A szabvány a bizalmi kapcsolatok között a különböző szintű csoportok közötti kapcsolatokat érti és így az alábbi hálózatokat különbözteti meg:

- hálózat ismeretlen felhasználói csoportokkal;
- hálózat ismert, kizárólag a szervezeten belüli felhasználói csoporttal;
- hálózat ismert, zárt üzleti csoporton (több szervezeten) belüli felhasználói csoportokkal.

Véleményünk szerint a katonai rendszerek átviteli út biztonságának szempontjából itt a különböző fontosságú kapcsolatokat kell beazonosítani, ennek okán elsősorban a vezetésfolytonosság biztosításában játszott szerepük szerint kell priorizálni az átviteli utakat.

3.3.2. Az átviteli út kockázatainak felmérése

A felmérés során az alábbi szakterületeken célszerű vizsgálódásokat lefolytatni a kitűzött cél eredményes elérése érdekében:

- vagyontárgyak azonosítása;
- fenyegetések azonosítása;
- sebezhetőségek azonosítása;
- létező ellentevékenységek felmérése;
- a kockázat bekövetkezési következményeinek azonosítása;
- a kockázatok becslése;
- a kockázatok kiértékelése.

3.3.3. Kockázatjavítás

A kockázatjavítás során dönthetjük el, hogy milyen ellenintézkedéseket tegyünk a kockázatok lehetséges következményeinek csökkentésére. Az ellenintézkedések lehetnek olyanok, amelyekkel teljesen elkerüljük a kockázatokat, illetőleg csökkentjük az események bekövetkezésének hatását vagy elkerüljük a kockázat előfordulását, valamint olyanok, amelyekkel a kockázatok negatív következményeit áthárítjuk egy másik félre [8]. Azt, hogy melyik ellentevékenységeket fogjuk alkalmazni az adott körülmények fogják eldönteni.

A kockázatjavítás során ki kell dolgozni azokat az ellenintézkedéseket, amelyeknek az értéke a kockázatok kiértékelésekor az elfogadható szint fölé került. Ezek az ellenintézkedések lehetnek technikai megvalósításúak és szervezésiek, valamint a kettő kombinációi.

Annak eldöntése, hogy milyen ellenintézkedéseket vezetünk be, függ attól, hogy milyen erőforrásaink vannak és milyen szinten kívánjuk megvalósítani az átvitel biztonságot.

3.3.4. Kockázatelfogadás

A kockázatok elfogadásának alapvetően két fajtája létezik. Az egyik esetében a kockázatelemzés folyamataként feltárt, kiértékelt és az ellenintézkedések érvénybe léptetésével olyan szintre csökkentettük a kockázatokat, amelyek már további intézkedést nem igényelnek, vagyis az elfogadható szint alá kerültek.

A második esetben a kockázatok létezésének tudatában vagyunk, de valamilyen okból nem tudatosan marad el intézkedünk a kockázat megszüntetésére.

Mindkét esetben azonban a kulcs szó a tudatosság, vagyis nem felelőtlenül abban bízunk, hogy a nem várt esemény nem következik be, hanem tudatában vagyunk a cselekedetünk teljes súlyával.

3.4. Incidenskezelés és vezetésfolytonosság tervezés

A végrehajtott, megfelelő szintű kockázatjavítás után a kockázatok csak a legritkább esetben szűnnek meg teljesen. A biztonsági állapot sehol nem annyira változékony, mint egy katonai feladat végrehajtása során, ezért a biztonsági környezetet folyamatosan figyelemmel kell kísérni. A biztonságban bekövetkezett negatív események hatásuk nagyságtól függően lehetnek:

- biztonsági események;
- biztonsági incidensek.

A katonai műveletek legnagyobb súlyú biztonsági incidense a vezetés megszakadása. A vezetés megszakadásának legvalószínűtlenebb forgatókönyve az egyszerre, hirtelen bekövetkező események hatása. Sokkal elképzelhetőbb, hogy több, akár egymástól független incidens sorozat eredményeként jutunk el a vezetés teljes hiányához. Ebből az okfejtésből is látszik, hogy nagy hangsúlyt kell fektetni a VIRTAR információbiztonsági incidenskezelésére.

Az átviteli út incidensei közé kell sorolni minden, az ellenséges tevékenységre utaló cselekményt, úgymint:

- berendezések támadása, rongálása;
- rádióforgalom zavarása, lefogása.

Szintén ebbe a kategóriába soroljuk azokat az eseményeket, amelyek az átviteli utak sávszélességének jelentős csökkenését okozzák az okok eredetétől (természeti hatások, ellenséges támadások, saját csapatok tevékenysége, stb.) függetlenül.

3.4.1. Az incidenskezelési terv

Az incidensek kezelése lehet ad-hoc jellegű, amikor a szakembereink meglévő szaktudására támaszkodunk, azonban célravezetőbb, ha elkészítünk egy incidenskezelési tervet. Természetesen minden eshetőséget nem tudunk feldolgozni, mivel előfordulhatnak váratlan,

eddig még nem tapasztalt események és incidensek, azonban egy meglévő terv sokat segíthet egy „éles” helyzetben.

Adaptálva az MSZ ISO/IEC TR 18044 szabvány 7. fejezetét véleményünk szerint az információbiztonsági incidenskezelési tervnek az átviteli út vonatkozásában az alábbiakat kell tartalmaznia:

- áttekintés az információbiztonsági esemény észleléséről, bejelentéséről, a lényeges információk összegyűjtéséről, valamint arról, hogy hogyan használják fel ezt az információt az információbiztonsági incidensek meghatározására. Az áttekintésnek tartalmaznia kell az információbiztonsági események lehetséges típusainak összefoglalását, azok bejelentési módját, azt hogy mit jelentsenek, hol és kinek és tartalmaznia kell azt is hogyan kezeljék az információbiztonsági események teljesen új típusait;
- az információbiztonsági incidensek bejelentésének folyamatát (ki a felelős, mi a teendő az esemény észlelésekor, bejelentésekor);
- egy információbiztonsági esemény információbiztonsági incidenssé történő átminősítését követően végrehajtott tevékenységek összefoglalása. Ennek tartalmaznia kell a következőket:
  - az azonnali megteendő intézkedések;
  - az incidens forrásának azonosítása;
  - mikor, milyen esetekben kell azonnal jelenteni az incidenseket a törzsfőnöknek vagy a parancsnoknak;
  - a másodlagosan megteendő intézkedések;
  - a felelősségek rögzítése;
  - az incidenskezelési tevékenység naplózási követelményei a későbbi elemzések számára, illetőleg az elektronikus bizonyítékok biztos megőrzésének biztosítása folyamatos megfigyeléssel;
  - az információbiztonsági incidenseket követő és megoldásukat szolgáló tevékenységek, beleértve a tanulságok levonását, valamint az eljárások megjavítását is;
  - az átviteli út rendszerdokumentációjának (beleértve az eljárásokat is) tárolási helye;
  - az információbiztonsági incidenskezelés oktatásának és képzésének feladatai.

3.4.2. A vezetésfolytonosság

A vezetés folytonosságának fenntartása a vezetés egységének egyik alapvető feltétele, így a sikeres tevékenység alapja. Az erők alkalmazásának időszakában a vezetés megszűnése a kitűzött célok elérésének meghiúsulását okozhatja. A parancsnok a műveletek teljes időszakára köteles megszervezni a helyettesítését, a vezetés átvételének rendjét. A vezetés folytonosságának fenntartása érdekében a feladatokat az alárendeltek részére úgy kell meghatározni, hogy az összeköttetés megszakadása esetén is garantálja a kitűzött célok teljesítését [9].

A legjobban megvalósított információbiztonsági ellenintézkedések, a legkiválóbban végzett információbiztonsági incidenskezelés ellenére is bekövetkezhet, hogy a vezető szervek valamilyen objektív oknál fogva nem tudják irányítani, vezetni az alárendeltjeiket. A vezetés megszakadása nem minden esetben csak a VIRTAR-ban bekövetkezett nem kívánt események következménye lehet, hanem más jellegű is, például a vezető szervek vezetésre képtelenné válása a vezetési pont megsemmisítése, vagy a vezetői állomány fogságba esése következtében. Ennél fogva a vezetésfolytonosság nem elsősorban a VIRTAR-t üzemeltető állomány feladata.

Gyakorlatilag az Összhaderőnemi Doktrínával megegyező az előzőekben már hivatkozott MSZ ISO/IEC TR 18044 szabvány meghatározásai is. A doktrínából az is következik, hogy az infokommunikációs összeköttetések teljes megszakadása sem feltétlenül jelenti egy katonai feladat kudarcát, ennek ellenére a VIRTAR üzemeltető állománynak mindent meg kell tennie azért, hogy a kor színvonalán álló, megfelelő sávszélességű csatornákat biztosítson a vezetés számára [10]. Áttekintve az átviteli utat biztosító személyzet feladatát, elmondható, hogy a szolgálati személyeknek:

- ismerni kell az általános helyzetet, miután ez nagymértékben kihat az összekötetések szervezésére;
- tisztában kell lenni, hogy ki, mikor, kit vezet, mert ez meghatározza az adott helyzet prioritásait;
- tisztában kell lenni, hogy az adott helyzetben milyen az infokommunikációs hálózat, milyen kerülő utakat tud elérni;
- tudni kell, hogyan lehet adott esetben a hírrendszerben átcsoportosításokat végrehajtani a kevésbé fontos csatornáktól a fontosabbak felé és természetesen tudni kell felállítani egy fontossági sorrendet az átvinni kívánt információk között;
- tisztában kell lenni, hogy melyek azok a minimális kommunikációs szolgáltatások, amelyek még biztosítják a vezetésfolytonosság infokommunkációs feltételeit.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Jelen közleményünkben megvizsgáltuk a VIRTAR információbiztonságának alapvető kérdéseit. Az információ és a szolgáltatások bizalmasságának, sértetlenségének, rendelkezésre állásának, letagadhatatlanságának, számonkérhetőségének, azonosíthatóságának és megbízhatóságának elvesztése igen káros hatással van a szervezet üzleti működésére. Következésképp az információk védelme és az informatikai rendszerek biztonságának menedzselése a honvédségi rendszerekben, ahol adott esetben (konfliktusok, missziók) emberéletek és akár a küldetés sikere is múlhat az információbiztonságon, kritikus fontosságú.

Az anyagban foglaltakat mérlegelve az alábbi következtetéseket vonjuk le:

- A VIRTAR-hoz kapcsolódó biztonsági területek kidolgozottsági foka az átvitelbiztonság részterületén tekinthető a legalacsonyabbnak;
- Az átviteli út biztonság feladatrendszerét a nemzetközi szabványok adaptálása révén célszerű meghatározni;
- A VIRTAR biztonságának fokozása érdekében incidenskezelési és vezetésfolytonossági tervet szükséges kimunkálni.

FELHASZNÁLT IRODALOM:

[1] MSZ ISO/IEC TR 13335-5 Informatika. Az informatikai biztonság menedzselésének

[2] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 16 § (4) bekezdés

[3] A honvédelmi miniszter 94/2009. (XI. 27.) HM utasítása a honvédelmi tárca információbiztonság politikájáról 22 §

[4] Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben I. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 110-121. oldal)

[5] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal)

[6] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal)

[7] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal)

[8] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE I. (Tábori és hordozható informatikai eszközök I.) (Hadmérnök on-line, IV. évfolyam, (2009) 2. szám, 333-339. oldal, ISSN 1788-1919)

[9] Négyesi Imre: TRAGBARE UND FELDINFORMATIK-GERÄTE II. (Tábori és hordozható informatikai eszközök II.) (Hadmérnök on-line, IV. évfolyam (2009) 3. szám, 355-362. oldal, ISSN 1788-1919)

[10] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05-06.)

Levente Szabó
szabo.levente@mil.hu

NETWORK AND SECURITY DEVELOPMENT WITHIN THE HUNGARIAN DEFENSE FORCES

Absztrakt

Ez a cikk a Magyar Honvédség Transzporthálózatát járja körül néhány gondolat erejéig, kezdve a hálózat kiépítésének első lépéseitől, a kezdeti nehézségeken át a kiépítés mögötti koncepcióig néhány technológiát áttekintve, amelyek a működéséhez elengedhetetlenül szükségesek. Továbbá szó lesz az informatikai biztonság szintentartásának nehézségeiről, valamint egyéb gondolatokról, amelyek ezen a területen fölmerülhetnek, úgy mint az informatikai biztonsági intézkedések szükségessége és okai.

This article describes a few thoughts on the IT Transport Network of the Hungarian Defense Forces. Starting from the actual network development, the difficulties it faced in the beginning and concept of development behind it, discussing some of the technologies used to achieve its functionality. It also discusses some of the challenges in maintaining security on the network and other aspects that may come to mind in this area, as well as the necessity to have IT security implementations and its reasons.

Kulcsszavak: *hálózatbiztonság, Magyar Honvédség, Transzporthálózat, hálózatfejlesztés, biztonsági tudatosság ~ network security, Hungarian Defense Forces, Transport network, network development, security awareness*

The development of Information Technology has been similar all over the world. Based on the structure of the several existing communication networks, something new emerged from the debts of a US Army laboratory, the ARPANET. This network was invented to be able to connect a few of the newly invented gadgets, the computers, and for them to able to work together in various forms. Only a few years have passed, and today we have the internet at our hands, with which we are able to visit libraries on the other side of the world, or work on the same projects with our colleagues being in distant places and possibly having access to no local infrastructure, communicating over satellite.

This boom of technology and the rate at which prices dropped allowed ordinary people to be a part of something brand new, something they have never experienced before. Unfortunately along with this freedom came something that was not necessarily foreseen. The fact that not only a selected few had access to computers like before emerged with the introduction of the PC. A lot of young and not so young fans of this new technical toy that they could put their hands on started to experiment with it. Where are their limits? What can they accomplish? This is the time when the first viruses were born, and when people started hacking into different, allegedly well protected systems, in most cases just for the fun of it. Unfortunately these types of activities quickly evolved into a very tempting attempt to earn money the easy way. Using peoples' inexperience with computers and the security gaps in the different systems, it did not take long before computer related crimes started costing a lot of people a lot of money.

Of course this just got worse with the development of the networks, the acquired speed, and the lost control, especially with the wireless area evolving very rapidly. It is amongst these threats and requirements that the IT network of the Hungarian Defense Forces started being built up. For some reason the existing communications infrastructure of the Army was not as rapidly exchanged with the new means of communication as those of the private sector. Of course there are financial reasons no one can put aside when planning the introduction of a completely new technology replacing the old one, especially if this existing infrastructure is seemingly working fine. Fortunately with time came the realization that the IP world can no longer be kept „out the door", and computers and networks started to appear within the Army's infrastructure.

At first these computers were just an experimental approach at data processing. The general idea was that all the means of communication and planning that exist at the moment are sufficient for answering future demands, but the computers can be used to free up manpower and energy by facilitating the processing of large amounts of data. This was of course an idea that was proven wrong relatively fast, and the importance of computers and computer networks grew with every minute. With this tendency came at first the development of the Budapest area infrastructure and hardware park. (As one might know, Hungary is very Budapest-centric in a lot of areas. The case happens to be similar with the Army, not necessarily because Budapest is considered as the most „important" city of the country, but simply because of the number of units in the area, compared to other regions of Hungary.)

Word was rapidly spread that this new technology really can offer an increase in productivity, whatever the task may be, especially by means of interconnecting several machines, so in other words communication was made possible by a new means, so far unknown to the general audience. This understanding led to the desire to be a part of this network, and so came the developments that made the Army's transport network that what it is today. Firstly some other main headquarters (like Székesfehérvár or Veszprém) were interconnected with the Budapest network, but as time passed and some more money was invested, the network development reached smaller units along the countryside as well. Of course the bandwidth that they had access to was usually nowhere near that of the HQ's, but nevertheless they were connected.

Needless to say this process is not finished, and it probably never will be, since there is an ongoing technological development that's offer of newer solutions by the day cannot be met at such a large scale of entities. There are still some segregated parts of the Defense Forces that need to be joined to the Transport Network, and generally it is a global interest to constantly develop the bandwidth at which the endpoints have access to it.

But what is this Transport Network anyways? It is a large network infrastructure interconnecting a fair amount of Local Area Networks built for a number of reasons, the most important of which are to assure communications between all parts of the network, and to be able to centrally manage, supervise and troubleshoot all network activity passing through to assure the confidentiality, integrity and availability of information at all times under all circumstances. This so called "CIA theory" is widely known amongst professionals from the IT field, and it signifies exactly what the defense sector is looking for in communications, that is the knowledge that the required information is always there when needed, seen only by those permitted and that it is legitimate, unaltered in other words secure. This network is also supported to our troops serving abroad via satellite shots.

In the Budapest are we have created an optical ring with 4 of the units stationed there attached, and the connections towards the other units vary between 100 Mbps and 2 Mbps, depending on their geographical placement and the number of hops between them and the uplink to the Transport Network. It lies in the interest of both the units sharing a lower amount of bandwidth and of those with a faster network access to develop this access speed as fast as possible to as high as possible, in order to assure the quality of communications both ways.

To have such an interconnected set of systems is good for both the user side and administrator side, since everyone is able to communicate with everyone else (of course with whom they are allowed to), and out of the other perspective this communication is controlled and regulated. Central management is a key factor in this, and so we try to develop this factor as much as we can by regulation if possible or by infrastructural development (by the acquisition of new hardware and/or software products).

This network is not called Transport Network by chance. It supports the transport of various services between the sites it interconnects, some of the more important of which are: internet, intranet, e-mail, voice over IP, video over IP and application virtualization. Easily guessed, this network supports only the IP protocol. (At this time only IP version 4, but in the future the implementation of IPv6 is likely to be considered.) One might begin to wonder how the internet and the local intranet of an organization such as the Hungarian Defense Forces can travel on the same network path. This technology has only been introduced a few years ago. Before that we had separate networking equipment for the types of networks, completely separating them physically, with no points of interaction made possible. Unfortunately this tendency had to be given up because of monetary reasons. It was simply too expensive to be putting two pieces of hardware everywhere, not to mention the cabling and the administration hassle.

Fortunately the MPLS[1] combined with VPN[2] technology was implemented and we were able to bring several separated networks “under one roof” so to say. This technology is based on the ability to flag packets which belong to different networks in a way that they can be separated at the receiving location with the assurance that they do not get mixed up along the way. These separated types of traffic have totally different routing rules applied to them (which they need since the IP addressing scheme is totally different), and to manage this, so called VRF’s[3] are created within the participating routers.

This type of virtualization affects our lives more and more each day. This technology allows us to reduce costs while delivering a wider range of services. For example this is how we support internet access to clients within in the intranet network. We use a controlled terminal server with all the necessary security means implemented, and we let our users connect to this, to view a virtual desktop with internet content on it. This way no physical connection is made between them and the outside network, but they still get the internet handed to them.

When it comes to security implementations, there are always to perspectives. One is that of the security professionals and the other is of the users, who fall under the new jurisdiction. Whether we talk about IT security or any other type of security implementation, for example installing a security guard at the entrance of an office to whom all workers must show their

1 Multiprotocol Label Switching
2 Virtual Private Network
3 Virtual Routing/Forwarding

badges upon entering and exiting the facility, the case is the same. There is a general discomfort against these newly created rules that make life harder for the employees. In case of the security guard, they would probably complain about having to look for their badges in the morning, barely having woken up and then again in the evening, when they are already late for their bus, etc. Of course these minor inconveniences tend to disappear when the guard stops a burglar from stealing all of the ID cards and wallets of the employees currently sitting in the office.

The case is no different in the IT world, whether we talk about civilian companies or government organizations. Naturally priorities are different, but the need to spend money on something that produces no "real" and "seeable" outcome is always something very difficult to explain. The situation was similar in the early phases of network buildup within the Defense Forces. All computer-related technology was new, and we didn't really know how to protect our valuable data and from what threats, so in the beginning there was virtually no protection at all. This changed when more and more computers were interconnected and unforeseen events, for example virus attacks started occurring. This was the beginning of the process that led to where we are today, and the knowledge that we must continue an ongoing development if we are to successfully handle all threats risking our networks.

As I mentioned before, the main goal is to keep the confidentiality, integrity and availability of all types of information that are transmitted through the network. Needless to say, with such a number of endpoints connected and services transmitted, this is by far not an easy task. And this does not only concern the physical protection of these networks from the outside world, or not to say threats coming from the inside. This protection needs to address a far greater field of understanding, namely the human participants of the network.

If you look up the definition of 'system' in a dictionary you will find something like this: [Organized, purposeful structure regarded as a 'whole' consisting of interrelated and interdependent elements (components, entities, factors, members, parts etc.). These elements continually influence one another (directly or indirectly) to maintain their activity and the existence of the system, in order to achieve the common purpose the 'goal' of the system][4]. When we talk about computer networks, it is impossible to forget that these networks do not function on their own, without user intervention, not to say that their goal of functioning cannot be determined without anyone to hand it to. The unfortunate fact is that the computer networks are so complex and hard to oversee nowadays that the actual users who interact with them have really no idea of what they are doing, and so become a danger in themselves to the system of which they are inevitably part of.

It is because of this that we have a double security perspective. On one side we have the technological aspects. We protect our networks with firewalls, IDS systems, anti-virus products, by the implementation of certain security focused group policies, etc. This keeps us secure up to some point, but we cannot forget the other (and in my opinion an even more important) aspect, the people using our IT infrastructure. If we educate people not to open suspicious links they got in e-mails, to regularly update their anti-virus products on their home computers as well, not to share personal information such as PIN codes with anyone, not to use the same passwords everywhere, etc., then we basically overcame most of the threats endangering our networks, before they even happened. This is why security focused training is regularly held by the professionals working in this area for the current users of the network, and IT security is something that the cadets attending our National Defense University have to get familiar with in order to pass their exams.

4 Taken from www.businessdictionary.com

The importance of this training has been demonstrated several times in the past by events that happened to occur. Without the claim of plenitude allow me to mention a few of these risks that we have to face. Nowadays the demand to work from any physical location arose in the defense community as well. This holds in itself two major risks at the same time. One is the question of mobile data carriers (pendrives, laptops, mobile phones, etc,) and the other is the key to mobility, wireless technology.

Pendrives (and I consider all other data carriers which use memory cards, such as digital cameras or voice recorders to be the same in this aspect) are very controversial gadgets. They are able to carry an immense amount of data, they are small, easily moved from one PC to the other, they are operating system independent, etc. On the other hand they are easily lost (carrying valuable corporate information), they can carry malicious programs from one network to the other (or even isolated workstations) and they somehow always tend to end up in the hands of the person we wanted to keep the information kept away from.

Laptops are similar to pendrives but they also carry on them an operating system with perhaps cached passwords or network information, plus they are nowadays by default manufactured to be able to communicate over a wireless network. The problem with these wireless networks is that it is virtually impossible to control access to them and because of this no matter how good our encryption methods may be, we can never know who is listening in on our traffic and from what distance.[5] You can find many ways to build long range antennas on the internet, with which you can capture all the traffic transmitted over a certain period of time. If this can later on be cracked by some method then the information we wanted to keep safe is obviously compromised.

Last but not least I would like to mention that our security system has to withstand the most dangerous threat that can appear, the malicious employees. It is by far the most difficult aspect of IT security, since we have to grant users certain permissions in order for them to be able to work, but we also need to be aware of what they are doing and to interfere if they try to do anything that they are not supposed to.

To conclude I would like to point out that security plays a key role in maintaining a certain level of services on our networks. Security is a state we can reach, but we need to adapt it at all times, since our networks exist in a constantly changing environment with emerging threats and changing attacking techniques which need to be neutralized in order to keep our systems safe. It has been a long development until we reached the complex IT network we have today, but this development never seized and is continuing as we speak. In order to reach an even better state of security we need to continue our network and security infrastructure development, our security focused trainings but whatever we do it always comes down to one major factor in the equation: money. Without the proper funding it is impossible to maintain a certain level of achieved security, not to mention developing it, so it is imperative that our decision makers are always aware of our work and of its importance.

5 For example: http://www.engadget.com/2005/11/15/how-to-build-a-wifi-biquad-dish-antenna/

USED LITERATURE

- Merike Kaeo, Designing Network Security, 2004, Cisco Press
- Saadat Malik, Network Security Priciples and Practices, 2003, Cisco Press
- http://www.networkworld.com/news/2009/122309-how-mpls-works.html
- http://www.businessdictionary.com
- http://www.engadget.com/2005/11/15/how-to-build-a-wifi-biquad-dish-antenna/

Papp Zoltán
pappz.szeged@gmail.com

RFID – ÚJ TECHNOLÓGIA VESZÉLYEI

Absztrakt

A 2001 szeptemberében történt new-yorki terrortámadások után egyfajta félelem alakult ki a világban. A média terrortámadásokról, repülőgép-óriásbombákról, állandó fenyegetettségről szóló híradásokkal gerjesztette tovább a már meglévő feszültséget az emberekben világszerte. A fejlett országok kormányzatai a terrorfenyegetettségre hivatkozva számos olyan biztonsági rendelkezést vezettek be, melyek célja az volt, hogy a potenciális elkövetőket kiszűrjék, mozgásukat, bejutásukat a nyugati világba megakadályozzák. Ezek az olykor kényszerintézkedésként is értelmezhető szabályok egy része a személyi szabadságjogok, a személyes adatok védelmének korlátozását is jelentették. A hatóságok eszköztárában egyik ilyen újdonság az elektronikus adatokkal ellátott útlevél lett.

After the terrorist attacks in New York in September 2001, a kind of hysteria unfolded internationally, the media was shocking the public with news and coverage of terrorist attacks, giant aeroplane bombs and constant threats. In reference to the terrorist threats, the governments of the developed countries have introduced several security measures aiming to filter potential perpetrators, block their movement and prevent their infiltration into the Western world. Some of these rules that may have been interpreted as forced measures have also meant a limitation on human rights and the protection of personal data. One of these new instruments applied by the authorities was the passport enhanced by electronic data.

Kulcsszavak: *személyes adatok védelme, rádiófrekvenciás azonosítás ~ protection of personal data, Radio Frequency Identification*

1. ábra: Elektronikus adatokkal ellátott útlevél

Az útlevél egyik borítólapjába egy úgynevezett RFID chip-et tartalmazó lemezkét ültetnek be, amelyet a külső oldal felől, a papír-műanyag kompozit borítóba elhelyezett árnyékoló fémháló véd az illetéktelen letapogatás ellen.

2. ábra: Az RFID chip lehetséges elhelyezkedése az útlevélben

Az RFID rövidítést a Radio Frequency Identification (rádiófrekvenciás azonosítás) szavak kezdőbetűiből képezték. Az RFID az egyedi azonosító technológiák (AUTO ID) családjába tartozik, hasonlóan a vonalkódokhoz, csak épp működési elvében tér el. Ez az automatikus azonosításhoz és adatközléshez használt technológia, melynek lényege adatok tárolása és továbbítása RFID címkék és jelolvasó eszközök segítségével. A chip köré épített áramkör a bejövő rádióhullámokból indukál áramot, így gyakorlatilag a leolvasó hozza működésbe az eszközt, és a benne lévő adatokat az egyben antennaként is funkcionáló áramkörön keresztül sugározza vissza a leolvasó egységnek. Az adatok általában egyszer kerülnek betöltésre, később már nem írhatóak át, azaz a leggyakrabban használt chip-típus az egyszer-használatos, eldobható. Az RFID címkéknek több típusa van, közös jellemzőjük, hogy rendelkeznek antennával. A címkéket elsősorban energiaellátásuk alapján különböztetik meg:

Passzív RFID

A passzív címkék nem tartalmaznak saját energiaforrást. Az olvasó által kibocsátott rádiófrekvenciás jel elegendő áramot indukál az antennában ahhoz, hogy a lapra épített apró, CMOS technológiával készült integrált áramkör feléledjen, és választ küldjön az adatkérésre. Az antenna tehát speciális tervezést igényel: nem elég, hogy összegyűjti a szükséges energiát, a válaszjelet is közvetítenie kell. A válaszjel általában egy egyedi azonosítószám, de előfordul, hogy a címke egy kisméretű memóriát is tartalmaz, ami lekérdezéskor ennek tartalmát is továbbítja az olvasó felé. Passzív címkék 125 kHz, 13,56 MHz, és UHF (860-960 MHz) tartományban működnek. Némely rendszer a 2,45 GHz-es sávot illetve egyéb sávot is használhat. A passzív lapkák rendkívül kisméretűek, jelenleg 0.4x0.4 milliméteres felületű, papírnál is vékonyabb címke a kereskedelemben kapható legkisebb darab. A passzív lapok hatótávolsága néhány méterig terjed, azaz ekkora távolságból olvasható ki a tartalmuk a használt frekvenciától függően. Alacsony előállítási költségének köszönhetően jelenleg ez a legelterjedtebb típus.

Fél-passzív RFID

A fél-passzív azonosítók annyiban térnek el a passzív társaiktól, hogy tartalmaznak egy apró, beépített elemet. Ez lehetővé teszi, hogy az integrált áramkör folyamatosan üzemeljen. Nincs szükség az antenna energiagyűjtő kialakítására, ezért azt adásra optimalizálják. Ennek köszönhető, hogy az ilyen típusú azonosítók válaszideje jobb, és az olvasási hibák aránya kisebb, mint passzív társaik esetén.

Aktív RFID

Az aktív RFID címkék vagy jeladók beépített energiaforrással rendelkeznek, melyek elegendő energiát biztosítanak bármilyen integrált áramkör üzemeltetéséhez és magához a jeladáshoz is. Nagyobb hatótávolságot és memóriakapacitást biztosíthatnak passzív változatuknál, némelyik még a vevő által küldött adatok rögzítésére is képes. A használt frekvencia általában 455 MHz, 2,45 GHz vagy 5,8 GHz és az olvasási távolság általában 20-100 méter. Néhány aktív címke impulzusszerűen üzemel, hogy takarékoskodjon az energiával, így akár 10 évig is képes üzemelni. A jelenleg kapható legkisebb aktív RFID jelző nagyjából fémpénz méretű.

Az RFID elvének megszületése a II. Világháború idejére tehető, amikor a radart feltaláló Sir Robert Watson-Watt vezetésével egy titkos projekt keretében a britek kifejlesztették az első aktív saját-repülőgép felismerő rendszert. Ennek előzménye az volt, hogy a radar rendszerek katonai felhasználását nagyban nehezítette, hogy a radarképernyőn megjelenő repülőgépekről a légvédelem nem tudta eldönteni, hogy melyik katonai erőhöz tartoznak, ami folyamatosan megnehezítette a radar készülékek adatainak értelmezését, illetve lehetetlenné tette a hatékony légvédelmi reagálást. A németek vették észre először, hogy ha a pilóta billegteti a repülőgép szárnyait, a gépről visszaverődő rádióhullámok által a monitoron megjelenő kijelzések megváltoznak. Ez a kezdetleges módszer nevezhető az első passzív RFID rendszernek, mely alkalmas volt egy objektum azonosítására. A britek azonban egy adót helyeztek el RAF gépeire, mely amint jeleket vett a hazai földi radarállomástól, egyedi azonosító jeleket kezdett visszasugározni, majd ezt a jelet a földi állomás érzékelve sajátként azonosította a repülőgépet. Ezzel a britek megalkották az első aktív saját repülőgép felismerő rendszert (IFF - Identify Friend or Foe). Az aktív RFID rendszerek azonosításának elve gyakorlatilag pontosan ugyanez.

Az RFID chip tetszőleges helyen rögzíthető, vagy be is építhető az azonosítani kívánt objektumba, ami lehet tárgy, például egy árucikk, vagy alkatrész, illetve lehet élőlény is, így akár egy ember is. RFID címkéket használnak már a nagy logisztikai cégek, alkatrész raktárak, áruházak stb. a vonalkód helyett, hiszen a tárgyakon nem kell megkeresni a vonalkód helyét az azonosításhoz, ami jelentős időmegtakarítással jár. A gyorsaság mellett nagy előny, hogy olcsó is, és a parányi méretéből adódóan apró tárgyak azonosítására is alkalmas.

Visszatérve kezdeti példánkhoz, az útlevelekhez, melyek esetében a passzív chip a szokásos, az útlevélben vizuálisan is megjelenített adatokon kívül más biometriai adatokat is tárolhat, melyek tipikusan a fénykép, az ujjlenyomat és a retinalenyomat lehet. Azt lehet mondani, hogy egy ilyen útlevél az adott személyt teljes hitelességgel azonosítja. Az ePassport, vagyis az RFID chip-et tartalmazó elektronikus útlevél bevezetését a terrorfenyegetettségre hivatkozva a fejlett világ egyre több országa eldöntötte, ami alól az Európai Unió tagállamai sem kivételek, így már Magyarország is alkalmazza ezt a technológiát. Az érintett országok az új technológia bevezetésére óriási pénzösszegeket áldoztak, ami azonban korántsem biztos, hogy arányban áll az általa kínált – sok szakértő szerint kétes – biztonsággal.

Független informatikai szakértők már a bevezetés megkezdése előtt is jelezték, hogy nem akkora a technológia biztonsága, mint azt a bevezető országok próbálják meg elhitetni állampolgáraikkal, ugyanis az e-útlevél is pontosan az lesz, aminek érdekében az RFID technológiát kitalálták: egy adatszolgáltató gépezet, amely kérésre készségesen kiadja az érintettek személyes adatait, például vámvizsgálatnál, a repülőtereken, illetve más hivatalokban.

Határátlépéskor a kinyitott útlevelet vizuálisan ellenőrzi a hivatalnok, miközben az utas ujjlenyomatát az ujjlenyomat olvasó modulon keresztül beszkenneli egy számítógép. Magasabb fokú biztonság esetén egy kamera a szivárványhártya mintázatát is rögzítheti. A nyitott útlevél RFID chip-jéből eközben a gép kiolvassa az információkat, melyeket összevet a szkennelt adatokkal, a hivatalnoknak egy képernyőre kivetíti az útlevél tulajdonosának fényképét, aki pedig eldönti, hogy az utas arca azonos-e a szkennelt fényképpel. Ez a procedúra szinte nem is vesz igénybe többlet időt a hagyományos útlevél ellenőrzéséhez képest.

Az ICAO, a Nemzetközi Polgári Repülési Szervezet az elektronikus útlevél használatával kapcsolatosan ajánlásokat is megfogalmazott, mivel nem osztotta a bevezetés mellett döntő országok optimizmusát, mely szerint az új típusú útlevél látványosan csökkenti majd a visszaélések számát.

Közelebbről megvizsgálva a technológiát, illetve annak felhasználási módját, az RFID chippel ellátott útlevél már közel sem tűnik olyan biztonságosnak. Egy nemzetközi konferencián egy Lukas Grünwald nevű német hecker az általa két hét alatt kidolgozott módszer segítségével saját útlevelén mutatta be, hogy teljesen legálisan és könnyen beszerezhető eszközökkel – laptop, RFID chipolvasó, üres RFID chip, chip-író – az útlevél adatai egy üres útlevél chipjére pillanatok alatt átvihetők.

Az tény, hogy az eredeti chip adatai nem írhatók át, tehát az ellopott, elvesztett útlevelet nem tudják közvetlenül felhasználni más személy biometriai adataival, viszont a tulajdonos személyiségét ellophatják. Ez azok számára lehet értékes zsákmány, akik valamilyen tiltólistán szerepelnek (például beutazási és tartózkodási tilalom alá esnek), viszont a megszerzett adatokkal a szabad mozgás lehetősége megnyílik számukra. Egy kis gondatlanságot, biztonsági rést kihasználva idegen adatokkal és egy kis szerencsével átjuthatnak az ellenőrzéseken.

Valójában azonban arra sincs szükség, hogy megszerezzék a kérdéses útlevelet. Akár egy táskába rejtett leolvasó segítségével gyakorlatilag észrevétlenül hozzájuthatnak az adatokhoz. Csak annyit kell tenni, hogy a leolvasót a „hivatalos” leolvasó közelébe kell jutatni. Amikor az útlevél kisugározza az adatokat a „titkos” leolvasó, - ha megfelelő távolságon belül van - szintén veszi és rögzíti azokat. Ezután akár a helyszínen egy gépkocsiban, vagy mosdóban is megírható az új chip, a kérdéses útlevél elektronikus klónja. A klónozási eljárás legnehezebb pontja talán az üres RFID chippel rendelkező biankó útlevél megszerzése, vagy egy hamisított útlevélben a chip és a fénykép kicserélése.

Azt tudjuk, hogy a terroristák minden eszközt felhasználnak akcióik végrehajtása során. A terrorista szervezetek fiatalabb generációinak felnövésével arra lehet számítani, hogy az új technológiákra elődeiknél már jóval fogékonyabb fanatikus fiatalok jelentősen ki fogják bővíteni a terrorizmus eszköztárát. Ennek a generációnak már nem jelent problémát a számítástechnika, a programozás, a telekommunikáció. Az RFID esetében klónozás egyszerűsége nem az egyetlen veszélyforrás. Az említett konferencián a Flexilis Inc. munkatársai bemutattak egy videofilmet, amely egy megdöbbentő kísérletet rögzített. A jelenlegi, nem megfelelő árnyékolással rendelkező útlevélmodell nem mindig rejti el az adatokat. Amennyiben táskában, zsebben kicsit megnyitva van az útlevél, annak adatai már kiolvashatók. A videofilm azt mutatta be, amint egy bábu zsebébe helyezett útlevél adatait egy szemeteskukába rejtett leolvasó kiolvasta, majd az adatok alapján egy detonátort indított el.

Egy leolvasó azonban beállítható úgy is, hogy akár csak egy nemzet útleveleire, vagy akár egyetlen kiválasztott személynek az adataira adjon csak jelet a detonátornak. Különböző megfontolásokból (például parkolási és autópálya díjbeszedés, sorompók mozgatása) ma már RFID chipeket szerelnek a járművekre is, így a fenti példához hasonlóan támadhatóak ezek is. Ettől kezdve a bombák akár személyre, járműre is szabhatók.

Az Európai Unió több tagállama már az RFID személyi azonosító kártya (személyazonossági igazolvány) bevezetését is tervezi, aminek az árnyékolása nincs még annyira sem megoldva, mint az útlevélé, így az adatok még könnyebben, még messzebbről kiolvashatóvá válnak. Elképzelhető, hogy a közeli jövőben az állampolgár egy ilyen személyi igazolvánnyal a zsebében belép egy épületbe, ahol az ajtóban nevén említve köszöntik, majd személyére szabott információkat kap egy kijelzőn. A kiolvasott adatok alapján a számítógép könnyen meghatározhatja, hogy a chip birtokosa melyik marketing-célcsoportba tartozik, így annak a csoportnak szánt multimédiás reklámot közvetíti, például a fiataloknak divatos ruhákat kínálnak.

Az RFID azonosítási technológia terjedése megállíthatatlan, az élet egyre több területén (raktározás, gyártás-ütemezés, biztonsági beléptető-rendszerek, postai és futárszolgálatok, légi szállítás, tömegközlekedés, elektronikus fizetőkártyák, háziállatok azonosítása) jelenik meg. Népszerűségét jelezheti az is, hogy 2006-ban az Egyesült Államokban, a Kaliforniai Egyetemen már RFID felsőfokú képzést is indítottak. Az RFID technológián alapuló azonosítási rendszerek tulajdonságaiból levezethetők a jogvédők aggodalmai is, akik víziói szerint, ha a kormányzat vagy a multinacionális cégek megfelelő szenzorokat helyeznek el az utcákon, különböző épületekben, járműveken akkor nyomon követhetővé válnak az állampolgárok, felderíthetővé válnak szokásaik, az általuk fogyasztott termékek, baráti vagy tágabb ismeretségi körük. Az RFID és más új technológiák a jogvédők szerint közelebb hozzák George Orwell 1984 című regényében már vizionált, a „Nagy Testvér szemmel tart” jelmondat valósággá válását.

FELHASZNÁLT IRODALOM

- Wikipedia (letöltve 2010. szeptember 17. (http://hu.wikipedia.org/wiki/RFID))
- Vonalkód Centrum - Az RFID technológiáról (letöltve 2010. szeptember 15. (http://www.vonalkodcentrum.hu/index.php?page=234))
- Turcsán Tamás - RFID - Mi mindent lát a Nagy Testvér? (letöltve 2010. szeptember 16. (http://nonstopuzlet.hu/rfid-mi-mindent-lat-a-nagytestver-20090216.html))

Jéri Tamás – Pándi Erik – Tóth András
jeri.tamas@gmail.com – pandi.erik@zmne.hu – toth.hir.andras@zmne.hu

A KOMMUNIKÁCIÓS INFRASTRUKTÚRÁKKAL SZEMBENI ROSSZAKARATÚ TEVÉKENYSÉGEK[1]

Absztrakt

Jelen közlemény az IT hálózatokkal szembeni támadások kérdéseit dolgozza fel.

This publication deals with questions related to attacks on IT networks.

Kulcsszavak: *IT hálózat, támadás ~ IT network, attack*

BEVEZETÉS

A támadás az erő kezdeményező alkalmazása harcban, egymással ellentétes viszonyban állók közt a kezdeményező számára a győzelem kivívására, azaz a kedvező kimenetel vagy döntés kicsikarására.[2] Az értelmező kéziszótár szerint tehát, a támadáshoz ellentétes viszonyban kell a feleknek állni, ahol az egyik fél - erő alkalmazásával - a kedvező kimenetel vagy döntés eléréséhez kezdeményez.

A hálózatok támadásának meghatározásához meg kell állapítani, hogy kik az egymással ellentétes viszonyban álló felek, és, hogy a támadó szempontjából mi számít kedvező kimenetelnek, és mi az „erő” alkalmazása?

A védekező fél az a természetes vagy jogi személy, aki a hálózat kialakításával az adatok hatékony kezelését, az információ hatékonyabb felhasználását és költségmegtakarítást kíván elérni. A támadó fél az a személy vagy csoport, aki a hálózat, vagy a hálózat bármely elemének rendeltetésszerű működését meg kívánja változtatni, a hálózatba jogosulatlanul be kíván jutni, a hálózatban fellelhető adatokat meg kívánja szerezni, vagy azokon változtatni akar. Az alkalmazott „erő” olyan, a támadó fél részére rendelkezésre álló képesség, tudás, mellyel támadó tevékenység végezhető.

A hálózatok támadása olyan tevékenység, mellyel a támadó a célhálózat valamely elemének rendeltetésszerű működését meg kívánja változtatni, abba jogosulatlanul be kíván jutni, a benne fellelhető adatokat meg kívánja szerezni, vagy azokon változtatni akar.

A hálózat elleni támadás jellegéből adódóan lehet fizikai vagy adatkapcsolati, forrását tekintve pedig külső vagy belső.

A támadáshoz szükséges tudás megszerzése általában hosszú évek kitartó munkája, a rendszerek működésének legmélyebb szintű ismeretével és nagyfokú programozási gyakorlattal társul. A támadási tevékenység kulcsa mégis a támadási képesség megszerzése. Értelmezhető olyan plusz információként, mely birtokában már végrehajtható a támadás.

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült
2 http://wikiszotar.hu/wiki/magyar_ertelmezo_szotar/Támadás

1. TÁMADÓK ÉS MOTIVÁCIÓIK

Vajon kik a támadók? A fenti meghatározásból kiindulva, a támadók olyan személyek, akiknek szándékában áll a hálózatok támadása és rendelkeznek a támadás végrehajtáshoz szükséges képességgel, tudással. A szándék alapvetően sok emberben megvan, de mégsem tudnak sikeres támadást végrehajtani, hiányzik az a plusz „erő", mellyel fölényt tudnának kiharcolni, a célba vett rendszer biztonsági mechanizmusaival szemben.

1.1. Támadók

A köznyelvben a hálózatok támadásához „értő" személyek a hackerek. A hacker kifejezés alatt olyan számítástechnikai szakembert értünk, aki bizonyos informatikai rendszerek működését a publikus avagy a mindenki számára elérhető szint fölött ismeri. A nagy tudású szakember mélyen ismeri a számítástechnikai rendszereket, ezáltal képes lehet egy adott rendszerbe „betörni" (azt illetéktelenül használni), avagy amennyiben valamilyen motiváció hatására cselekszik, képes onnan információt a saját maga vagy mások számára eltulajdonítani.[3]

Ez persze még nem jelenti azt, hogy egy hálózatba csak és kizárólag hacker képes bejutni, hiszen a helyi ismerettel rendelkező volt rendszergazda, ideig-óráig információ fölényben van egy nagy tudású, ugyanakkor szűz területet „meghódítandó" hackerrel szemben.

A hackerek alapvetően két csoportba oszthatók:

- 'White-hat hacker'-nek (fehér kalapos hacker) nevezzük azokat a kiemelt tudással rendelkező informatikai szakembereket, akik tudásukat arra használják fel, hogy megbízás alapján vagy állandó jelleggel biztonsági hibákra világítsanak rá, ezáltal elkerülve és megelőzve a black-hat hackerek betörési kísérleteit.[4]
- 'Black-hat hacker'-nek nevezzük azokat a hackereket akik tudásukkal visszaélve, jogosulatlanul számítógépbe illetve számítógép-hálózatokba törnek be haszonszerzés, vagy károkozás céljából.[5]

A hálózatot támadók tehát két csoportba oszthatók:

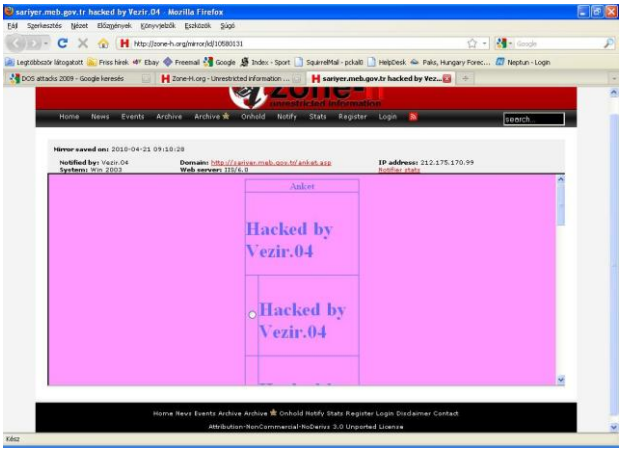
- hackerek (White-hat, Black-hat);
- a hálózat működéséről, vagy a hálózatban kezelt adatokról olyan plusz információval rendelkező személy, akit ezen információ, képessé teszi a hálózat megtámadására.

1.2. A támadások motivációi:[6]

- információ megszerzése (személyes, üzleti, katonai, stb.) haszonszerzés vagy károkozás céljából;
- szolgáltatásokhoz való illetéktelen hozzáférés (pl. nyomtatni, filmeket letölteni);
- szolgáltatások megbénítása;
- rendszer feltörése;
- rosszindulatú program(ok) bejuttatása;

3 http://hu.wikipedia.org/wiki/Hacker
4 http://hu.wikipedia.org/wiki/Hacker#White-hat_hacker
5 http://hu.wikipedia.org/wiki/Hacker#Black-hat_hacker
6 Póserné Oláh Valéria – Számítógép-hálózati támadások

- szórakozás, versengés pl. egy weboldal feltöréséért;
- politikai okokból;
- kifejezetten bűnös céllal (szerencsére csak kevés).



1. ábra: Deface[7]-elt Weboldal
Forrás: http://zone-h.org/mirror/id/10580131

2. TÁMADÁSI CÉLPONTOK, A KÁROKOZÁS LEHETSÉGES NAGYSÁGRENDJE

A támadás szándéka, módszere, lehetősége nagyban meghatározza a támadás célpontját, ezzel parallel módon az okozható kár nagyságát is. Az is mértékadó, hogy a hálózat pontjait mennyire egyszerű vagy bonyolult támadni, hisz sok esetben, több lépcsőben kisebb befektetéssel könnyebb elérni a célponthoz, mint egy lépcsőben, irreálisan nagy munkával vagy költséggel.

A támadások motivációiból kiindulva elmondható, hogy az valamely szolgáltatással van összefüggésben, tehát végeredményben szerver elérése a cél, mely - zárt - belső hálózatban, vagy az Interneten kiszolgálóként egyaránt üzemelhet. Hasonlóan a hétköznapi környezethez, a kibertérben is a legkönnyebben támadható célpontokat fogják először ostromolni, és azok közül is, a legkevésbé védetteket. Az Internetes kiszolgálóként működő szerverek elérhetősége a lehető legegyszerűbb, így nem véletlen, hogy azok támadása és feltörése a leggyakoribb. A szerverek elleni támadásoknak mégis gyakran a munkaállomások a kulcsfigurái. Egy észrevétlenül elejtett és irányítás alá vont munkaállomás megfelelő eszköz a tényleges, szerver elleni támadáshoz. A munkaállomás alapvetően is rengeteg – a támadó számára – fontos információt tárolhat, azonban – fertőzöttsége esetén - a vele végzett tevékenység tálcán kínálja azt az információt, mellyel a támadót képessé teszi a következő lépcső, azaz a szerverek elejtésére.

A támadással okozott kárt nagyban meghatározza a szerverről kinyert adat, információ értéke, érzékenysége, fontossága, vagy a szerver leállásával okozott veszteség. Minden természetes vagy jogi személynek vannak féltve őrzött adatai, amiket szeretne csak és kizárólag magáénak tudni. Előre nehéz meghatározni a károkozás nagyságrendjét, de leszögezhető, hogy a minimálistól a felbecsülhetetlen értékűig mindkét szélsőség előfordulhat.

Igazán komoly kihívást az jelent, amikor a szolgáltatás jellege igen érzékeny adatokra terjed ki, ugyanakkor a nagyobb profit elérése miatt elvárás a tevékenység működtetése (pld.

7 Weboldal tartalmának megváltoztatása támadással

e-bank világhálón keresztül). Ebben az esetben nagyon nagy a támadók csábítása, viszont a szolgáltatás működtetésének profitja biztosítja a támadások elhárítására fordítható költséget. Legutóbb világméretű botrányt kavart, amikor egy web-szerverről bankkártya adatokat loptak el, s éltek vissza velük, dollármilliókban mérhető kárt okozva a banknak, s a bank ügyfeleinek.

Fő támadási célpontok:

- Eszközök:
    a) Interneten – távoli adminisztrációval - működő szerver;
    b) Félig nyitott hálózatban működő szerver, kliens;
    c) Zárt hálózatban működő szerver, kliens.
- Alkalmazások;
- Kiszolgáló program;
- Operációs rendszer.

Az operációs rendszer sikeres támadása nagyobb „eredménnyel” kecsegtet, mert a rajta működő összes szolgáltatás működése befolyásolható.

3. A TÁMADÁS ESZKÖZEI

Az emberi dimenzióhoz hasonlóan, a kibertérben sem lehet ad-hoc jelleggel, előkészületek nélkül támadást vezetni. Egyrészt fel kell térképezni a támadandó hálózatot, majd a kellő információ birtokában, a megfelelő eszközzel végre kell hajtani a támadást, ezért megkülönböztethetünk információszerzésre és támadásra szolgáló eszközöket.

3.1. Információszerzés

Minden olyan, a célhálózattal kapcsolatos információ megszerzésére irányuló tevékenység, mellyel a támadási képesség elérhető.

Minden rendszer annyira erős, mint a benne található leggyengébb láncszem, ezért általában ezeknek a gyenge pontoknak a felkutatása a fő cél.

3.2. Információszerzés típusai:

- Közvetlen: célzott információszerzés a megtámadandó – szolgáltatást nyújtó – szerverről. (pld. szerveren futó szolgáltatások);
- Közvetett: olyan információ megszerzése, mely felhasználásával a közvetlen, vagy újabb közvetett információszerzésre nyílik lehetőség. (pld. munkaállomás operációs rendszere, melyről csatlakoznak a szerverhez).

3.3. Információszerzés eszközei

Social engineering

Nem más, mint annak a művészete és tudománya, hogy miként vegyünk rá személyeket arra, hogy a mi akaratunknak megfelelően cselekedjenek.[8]

8 Krasznay Csaba - A rendszer próbája: az etikus hackelés és penetrációs tesztelés (előadás)

A fentebb említett, szolgáltatási tevékenységben szereplő emberi tényező kiaknázásáról van szó, hisz nem szükséges bonyolult eszközökkel a hálózatot vizsgálni, ha a kulcs információk a felhasználótól – apróbb cselekkel – megszerezhetők. Kevin Mitnick a legendás hacker, „A megtévesztés művészete" című könyvében számos példát mutat arra, hogy miként tudta rávenni a célhálózatban dolgozókat, hogy számára a támadáshoz szükséges információkat kiadják.

Saját tapasztalatainkból - is - tudjuk, hogy egy hálózat rendelkezhet bármilyen erős védelemmel, ha a felhasználók nem tartják be a biztonsági előírásokat, a rendszer támadható. Alkalmazható SE eszközök:

- direkt telefonos megkeresés (nevek, elérhetőségek, azonosítók, munkaidő-beosztás, esetleg jelszavak megszerzése);
- célzott levél (nyereménylehetőséggel „csak egy űrlap" kitöltetése hasznos adatokkal);
- kukaátvizsgálás;
- shoulder surfing – vállszörf (váll feletti információszerzés, pld. jelszó begépelés).

Információgyűjtő programok

Minden olyan program, vagy általa generált állomány, mely közvetlen, vagy közvetett információszerzésre ad lehetőséget. Segítségükkel hálózatvizsgálatot, adatforgalom lehallgatást, vagy gyűjtést végezhetünk. Működési elvük szerint, kontroll-alatt tartott, vagy a célzott helyre bejuttatott információgyűjtő programokat különböztetünk meg.

- kontrollált:

A támadó maga dönti el, hogy mikor indítja, meddig használja, és mikor állítja le a program működését. A legideálisabb eszköz, előnye, hogy a gyűjtött információ – az állandó felügyelet miatt - azonnal rendelkezésre áll. Zárt vagy félig nyitott hálózatok megfigyelése nehezen megoldható velük, mert az irányítónak, a programnak és megfigyelt eszköznek homogén hálózatban kell lennie. Tipikus alkalmazások:

a) port scanner – nyitott (TCP, UDP, ICMP) portok felderítésére;
b) sniffer – szaglászó a fontos adatok (pld. jelszavak) elfogására.

- bejuttatott programok:

A hétköznapi számítógép felhasználók számára még konkrétan beazonosítatlan az a „vírus" fajta, amit a vírusfigyelők csak ritkán találnak meg, ugyanakkor „a számítógépet nagyon lelassítja, főleg az Internetezés ideje alatt". A felhasználói oldalon sokszor csak apróbb kellemetlenségként könyvelik el, hisz minden működik, csak kicsit lassabb a számítógép, míg a „sötét" oldalon az egyik legnagyobb fegyver a kémprogram. „Kémprogramnak (angolul spyware) nevezzük az olyan, főleg az interneten terjedő számítógépes programok összességét, amelyek célja, hogy törvénytelen úton megszerezzék a megfertőzött számítógép felhasználójának személyes adatait."[9] Az információszerzés szempontjából létjogosultsága abban van, hogy a nehezen bevethető - zárt - hálózatokból a támadó személyes megjelenése nélkül is képes kinyerni az információkat. Alkalmazásuknak négy fő mozzanata van:

a) az információgyűjtéssel, rejtőzködéssel, információtovábbítással (esetleg szolgáltatási funkcióval) ellátott program elkészítése;

9 http://hu.wikipedia.org/wiki/Kémprogram

b) bejuttatása a zárt hálózaton belüli számítógép(ek)re;
c) a program működtetése;
d) az összegyűjtött információk kijuttatása a hálózatból.

A feladat minden pontját nehéz megvalósítani, ugyanakkor mindegyik szükséges az információ sikeres megszerzéséhez, azonban a leghangsúlyosabb - talán - a zárt hálózatba történő bejuttatás. A programok bejuttatása alapvetően két módszerrel lehetséges:

- beküldés
  - a belső hálózat valamely – kevésbé védett - szolgáltatását kihasználva (pld. email, chat);
  - ajándékként (pld. kulcstartó formájú pendrive-on).

- a belső hálózat valamely felhasználója, gyanútlanul letölti az Internetről a munkaállomására

A két megoldás ötvözve is előfordul, amikor a gyanútlan felhasználó - úgynevezett - rávezető email-t kap, melyben a meglátogatandó „hasznos" weboldal linkje szerepel, ahonnét óvatlanul letölti a programot. A kémprogramot gyakran álcázzák, legtöbbször egy másik – érdekes – szoftver részeként hozzák működésbe (pld. játékprogram). Tipikus alkalmazások:

- keylogger – billentyűzetfigyelő;
- rosszindulatú programok (kémprogram, trójai, vírus);
- távoli adminisztrációt biztosító programok.

A kontrollált és a bejuttatott program között átfedést jelent az a bejuttatott programfajta, mely képes a célszámítógép felett átvenni az irányítást (zombivá tenni), majd szolgáltatási funkciót indítva, kontrollálható programként működni. Ez a támadó részére a legbiztatóbb eredmény, míg a hálózat tulajdonosára nézve az egyik legnagyobb veszély, mert a hálózat - könnyen - teljesen kiszolgáltatottá válhat.

Nyilvános információk

Nagyon sokszor nyilvánosan, különösebb befektetés nélkül is elérhetők információk, melyek segítik a támadást, vagy következtetések vonhatók le belőlük. Ahogy fentebb is jeleztük, a cégek, hivatalok saját weboldalakat tartanak fenn az Interneten, ahol jó eséllyel megtalálhatók a fontosabb beosztásban dolgozók nevei, elérhetőségeik, email címeik. Hasonlóan lekérdezhető a hivatali munkarend, a nyitva tartás, a cím, stb. Ezek az adatok jó kiindulópontot jelentenek egy ügyes social engineering-ben járatos személynek, aki ügyes kérdésekkel pillanatok alatt további hasznos információkat szerezhet. Gyakori jelenség, hogy az email címek valamilyen származtatása (néha ugyanaz) egyben szerver hozzáférési azonosító is, mely szintén jó kiindulási pont a támadáshoz, de gyakran az egyszerű email is hasznos információkat hordoz. A célhálózat felhasználójának küldött érdeklődő email válaszából – általában - következtetni lehet:

- a levelező kliens programra;
- a munkaállomás operációs rendszerére;
- a levelező szerverre;
- a hálózatban preferált operációs rendszerekre, programokra;
- az előzőekből, a – nyilvános, kikereshető – gyengeségekre, támadási pontokra.

Ugyancsak hasznosak lehetnek az ingyenesen használható műholdképek, térképek, melyekkel információ szerezhető a célpont elhelyezkedéséről, kiterjedéséről, és valószínűsíteni lehet a hálózat nyomvonalát.

Kapcsolódás a hálózathoz

Az információszerzés szempontjából kiemelkedő lehetőség, a célhálózathoz történő csatlakozás. Ennek megvalósításával a támadó fél, kontrollált programokkal, viszonylag lebukásmentesen képes információt gyűjteni a hálózatról. A célhálózathoz kapcsolódni alapvetően kétféle módszerrel lehet:

- Fizikai kapcsolódás

Számtalan hálózati betörés oka a szabadon hagyott végpont, vagy aktív hálózati eszköz volt. Ekkor a támadó egyszerűen csatlakoztatja – információgyűjtő programokkal felszerelt – számítógépét a hálózathoz, és megpróbál aktívvá válni, hogy az adatforgalomból információkhoz jusson.

- Vezeték nélküli kapcsolódás

A WLAN (wireless LAN) rádióhullámot használó vezeték nélküli helyi hálózat, ami szórt spektrum vagy ortogonális frekvencia-osztásos multiplexálás technológia segítségével lehetővé teszi a közeli számítógépek összekapcsolódását.[10] Kétségtelenül nagyon hasznos és kényelmes eszköz, mára cégek és háztartások egyaránt nagy számban használják. Alkalmazásával megspórolható a kábelezéssel járó költség és vesződés, ezért kézenfekvő népszerűsége. A sok-sok előnye mellett van hátránya is, mely legfőképpen a biztonságosságában fedezhető fel. A rádióhullámoknak nem lehet megállj-t parancsolni, a falakon kívülre is kijut(hat)nak, ezáltal – a hálózat törvényszerűségei szerint – mások számára is rendelkezésére állnak. A támadó fél a vezeték nélküli hálózatok adatforgalmából rengeteg hasznos információt képes összegyűjteni titkosított kommunikáció esetén is, azonban a kulcs megszerzésével, vagy védelem nélküli kapcsolat esetén könnyen a hálózat teljes jogú tagjává válhat.

A szolgáltatás, alkalmazás gyengeségei

Előfordul, hogy a rosszul konfigurált, vagy biztonsági rést tartalmazó szolgáltató program, illetve a szükséges ellenőrző algoritmusok nélküli alkalmazói program juttatja információhoz a támadót:

- CGI – Common Gateway Interface

Web-szerver segítségével, bináris programok, vagy script-ek végrehajtására ad lehetőséget dinamikus weboldalak készítéséhez. Figyelmetlen beállításával az operációs rendszerről jeleníthetők meg adatok böngészőn keresztül, többek között a felhasználók azonosítóit, jelszavait tartalmazó állományok is.

- Sendmail

Az egyik legismertebb és legellentmondásosabb levelezőszerver. Hosszú időn keresztül nem is ajánlották használatát, mert súlyos biztonsági réseket tartalmazott. Egyik ilyen gyenge pontja volt, hogy kellően hosszú email cím használata esetén, memória túlcsordulással megállt és rendszeradminisztrátori jogosultsághoz segítette a levél küldőjét.

10 http://hu.wikipedia.org/wiki/WLAN

- SQL-Injection

Olyan dinamikusan, adatbázis értékekkel előállított weboldalak esetén alkalmazható, amikor a böngésző által küldendő változókból (POST, GET) származtatják az SQL parancsot. A változókon keresztül kiadott – célzott – SQL injekcióval az adatbázis-szerverből kinyerhetők a hőn áhított adatok (pld azonosítók, jelszavak stb..).

- Exploit (kihasználás)

Az exploit egy olyan kód (vagy bináris), amelyet a rosszindulatú támadó felhasználva kihasználhatja bizonyos programozási hibával rendelkező programok sebezhetőségét. Az exploitok egy részét nagy tudással rendelkező biztonsági szakemberek készítik, másik részét szintén nagy tudással rendelkező, rossz szándékú programozók. Ezek az emberek nem tévesztendőek össze az exploitokat letöltő, lefordító, és azokat rossz célra felhasználó, de emellett kis (vagy semmilyen) tudással rendelkező script kiddie-kel.[11]

Nyugodtan nevezhetjük a hackerek „csodafegyverének", hisz ezekkel a kódokkal – is – tanúbizonyságot tesznek kivételes tudásukról. Egy exploit megírásához először fel kell fedezni a cél program (pld. böngésző) sebezhetőségét, majd annak kihasználására el kell elkészíteni a kódot. Alapvetően kétféle exploitot különböztetünk meg:

- alkalmazott (a közvélemény által ismert);
- alkalmazásra váró.

A már alkalmazott exploitokra a gyártók - általában - adnak ki hibajavítást, azonban a frissítések alkalmazása nélkül könnyen védtelenné válhatnak programok. A bevetésre váró exploitok manapság nehezebben –, vagy sehogy sem – kerülnek napvilágra, mert a szoftveróriások nagy összegeket hajlandók adni egy-egy programban felfedezhető biztonsági résért, mely inkább kifizetődő a hackereknek, mint az ingyenes „népszerűség".

A sebezhetőség kihasználásával, - a programon keresztül - átvehető az irányítás a számítógépek felett, és a támadáshoz szükséges információ szerezhető meg.

3.4. Támadó eszközök

Az információszerzés és a támadás – sokszor – élesen nem választható el egymástól, előfordulhat, hogy a két tevékenység egyszerre, vagy egymással szoros összefüggésben zajlik.

- szolgáltatást bénító eszközök (DOS, DDOS)
  - SYN-árasztás;
  - ICMP-árasztás;
  - Halálos ping;
  - Erőforrások felemésztése.

- hamis megszemélyesítésre, jogosultság szerzésre szolgáló eszközök
  - jelszó visszafejtő - john the ripper;
  - lehallgató – sniffer;
  - billentyűzet figyelő – keylogger;
  - hoszt - azonosító - hamisító – IP spoofing.

- kártékony programok
  - vírusok;
  - trójai programok;

11 http://wiki.hup.hu/index.php/Exploit

    - férgek.

- hálózati elemeket támadó lehetőségek
    - ARP mérgezés;
    - forrás routolás;
    - kapcsolat elterelés;
    - routerek támadása;
    - fizikai hozzáférés.

4. A TÁMADÁS FOLYAMATA

4.1. Kutatás, felderítés

A hálózat minden részletére, elemére, alkalmazójára kiterjedő adatgyűjtés. A bűnüldöző szervek véleménye, hogy a világi értelemben vett betörések sikeressége, és a kutatásra, felderítésre fordított idő egyenesen arányos. Véleményünk szerint ez a feltételezés hasonlóan igaz a számítógép-hálózatok elleni támadások esetén is, tehát minél részletesebb, precízebb a feltárás, annál nagyobb esély van sikeres támadás végrehajtására. A felderítendő elemek:

- Hálózati infrastruktúra
    - kiépítettsége;
    - jellege, struktúrája;
    - fizikai védelme;
    - áramellátása;
    - Internethez kapcsolódása.

- Szerverek
    - operációs rendszerei;
    - szolgáltatásai;
    - elhelyezése;
    - mentési gyakorlata;
    - adminisztrálása.

- Kliensek
    - operációs rendszerei;
    - szervezeti alkalmazásai;
    - irodai alkalmazásai;
    - frissítésének gyakorlata.

- Alkalmazottak
    - életkor szerinti megoszlása;
    - létszáma;
    - nemek szerinti megoszlása;
    - informatikai oktatási gyakorlata;
    - fluktuációja;
    - munkarendje;
    - Internet hozzáférése.

4.2. Kiértékelés, gyenge pont(ok) kiválasztása

A felderített elemekből a leggyengébb láncszem és a támadási célpont kiválasztása.

4.3. Információszerzés

A gyenge ponton keresztül, a sikeres támadáshoz szükséges, közvetett vagy közvetlen információk megszerzése.

4.4. Támadás

A megszerzett információk alapján a támadási tevékenység céljának elérése, a rendelkezésre álló támadási eszközökkel.

4.5. Nyomok elfedése

Miután a hálózatok elleni támadás - általában - a büntető törvénykönyvbe ütköző magatartás, a támadónak célja megakadályozni, hogy tevékenysége és személye visszakereshető legyen. Napjainkban – szinte – minden szolgáltatás naplózással működik, ezért fontos tudni, hogy a nyomok hol keletkeznek, miként s mekkora energia ráfordítással tüntethetők el. A nyomok elfedésének lehetőségei operációs rendszertől függően a

- history állományok;
- registry bejegyzések;
- log fájl bejegyzések módosításával.

5. TAPASZTALATOK

A következő két eset leírásával, saját tapasztalatainkat szeretnénk bemutatni, melyek csak és kizárólag segítségnyújtási szándékkal, az érintettek tudomásával kerültek végrehajtásra.

5.1. Elfelejtett – email – jelszó

Egyik barátunk, akinek a számítógépeit rendszeresen karbantartjuk, felkeresett, hogy legyünk segítségére új gépe levelező kliensének beállításával kapcsolatban.

Otthoni – két számítógépből álló – mini hálózatából router segítségével használja az Internetet, leveleit pedig a szolgáltatótól kapott e-mail címére fogadja, melyeket Outlook Express (továbbiakban: OE) levelező klienssel, POP3-as protokollal tölti le. Barátunk kényelmes típus, nem igazán kedveli a jelszavak állandó begépelgetését, ezért ahol csak lehet, a „jelszó megjegyzése” lehetőséget alkalmazza. Ő is a digitális világban szocializálódott, és rendelkezik legalább 20 különböző kóddal vagy azonosítóval és az azokhoz tartozó jelszóvariánsokkal, melyeket már össze-vissza változtatott.

Már az új gépével szerette volna leveleit megnézni, azonban képtelen volt kitalálni e-mail címéhez tartozó jelszavát, az általa kipróbáltak egyike sem volt megfelelő. A szolgáltató hot-line ügyfélszolgálatával nem tudott zöldágra vergődni, melynek miértje túlmutat e cikk keretein, majd több órányi próbálgatás után hívott, hogy segítsünk.

A problémát átgondolva, lehetséges megoldásként a jelszó elkapás módszerét ajánlottunk, melyet barátom nagy örömmel fogadott el.

Az alábbi lépésekkel oldottunk meg a problémát:

- Linux operációs rendszerrel és sniffer programmal telepített laptopot a hálózatba kapcsoltuk;
- a laptop IP címét a régi számítógép tartományába állítottuk;
- a sniffer programot a régi számítógép IP címének és a 110-es TCP port figyelésével indítottuk el;
- a régi számítógépen a levelek letöltését kezdeményeztük az OE programmal;
- a sniffer programmal gyűjtött adatokat elemeztünk, melyben a levelek letöltéséhez szükséges azonosító után, megtaláltuk a jelszót;
- A megvalósításhoz kellett, hogy barátunk;
- megengedje, hogy a hálózatába kapcsoljuk a laptopot;
- titkosítás nélkül töltse le leveleit.

5.2. Elfelejtett WLAN jelszó

Barátom, vezeték nélküli hálózatába új laptopot szeretett volna csatlakoztatni, ezért, mint a család mindenes informatikusát hívott, hogy oldjuk meg a problémát.

Kényelmes ember és megszállott Internetező lévén, évekkel ezelőtt vezeték nélküli hálózat kialakításával bízott meg minket, hogy notebookjával a háza minden részéről tudjon böngészni a világhálón. A belső hálózatból WLAN router biztosítja az átjárást az Internet felé, melyre WPA (Wireless Protected Access) titkosítással lehet kapcsolódni. A jelszavak a router-en és a notebook-on egyaránt mentésre kerültek, majd szépen lassan a feledés homályába merültek.

Az új notebook WLAN hálózatba kapcsolásához szükségünk lett volna a nyolc karakter hosszú jelszóra, melyre sajnos már senki sem emlékezett. A router közvetlen kábeles konfigurálása megoldható lett volna, azonban egy olyan nehezen megközelíthető helyre került felszerelésre, hogy alternatív megoldást kerestünk a jelszó kitalálására.

Több esetben hallottuk már a vezeték nélküli kapcsolatok biztonsági kockázatairól, ezért – is – kíváncsiak voltunk a feltételezések igazságtartalmára.

A feladat megoldására a laptopot, egy SMC típusú – pcmci-os – WLAN kártyát, valamint egy nyílt forráskódú – vezeték nélküli – hálózatfigyelő-, analizátor programot használtunk.

A jelszóvisszafejtés menete a következő volt:

- a WLAN kártyát, figyelő (monitor) üzemmódba helyeztük;
- Ezzel lehetőség nyílt a hálózati forgalom figyelésére, scannelésére.;
- A - monitor üzemmódba helyezett - vezeték-nélküli interfészen keresztül a hálózati forgalmat összegyűjtöttük, mellyel információt szereztünk a router és a kliens:
    - MAC címéről;
    - jelerősségéről;
    - csatorna számáról;
    - maximális adatátviteli sebességéről;
    - alkalmazott titkosítási típusáról;
    - titkosító algoritmusáról;
    - vezeték nélküli hálózati nevéről.

A kommunikáció adatait folyamatosan gyűjtöttük és egy állományba mentettük.

- A router és a kliens között a WPA titkosítás egy PSK[12] típusú minimum nyolc karakteres jelszóval történik, melynek megszerzése egyben a feladat megoldása is. Miután a kulcscserére a kapcsolódáskor kerül sor, ezért egy már felépített

12 http://hu.wikipedia.org/wiki/WPA - Pre Shared Key / Osztott kulcs

kommunikáció esetén ki kell kényszeríteni, a megismételt kulcscserét, vagy meg kell várni az újra kapcsolódást. A kikényszerítésre legfőképpen Linux alatt van lehetőség, amikor a támogatott hálózati kártya segítségével csomagokat lehet beszúrni a hálózati forgalomba, azaz injektációt lehet végrehajtani. A kikényszerítésre nem volt szükségünk, hiszen a lehallgatandó notebook rendelkezésre állt, így csak egy egyszerű újrakapcsolódást hajtottunk végre, miközben saját laptopunk gyűjtötte az információkat. Az újrakapcsolódás után a gyűjtött adatok közé – kódolt formában - bekerült a titkosításhoz használt jelszó is.

- A jelszó visszafejtése brute force[13] módszerrel, azaz egy szótár alapján -, a próbálgatás módszerével – történt, melyhez a jelszót – is - tartalmazó dump állományt, valamint a betűk különböző variációs lehetőségeit tartalmazó szótár állományt használtuk. A brute force alkalmazásához a nevéből is kitűnő nyers erőt, azaz nagy kapacitású szervert használtunk, mely teljes hardver kihasználás mellett, két nap alatt találta meg a jelszót.
- A jelszó ismeretében már az új notebookkal is képesek voltunk a routerhez kapcsolódni, és számunkra is bizonyítást nyert, hogy a vezeték nélküli hálózatnak is vannak gyenge pontjai.

A bemutatott két esetben ugyan jó célra, de mégiscsak – a hétköznapi emberek számára is ingyen letölthető – támadó eszközöket használtunk. A második esetben bemutattuk, hogy miként lehet biztonságosnak hitt vezeték nélküli hálózathoz kapcsolódni, az első esetben pedig arra világítottunk rá, hogy a hálózathoz kapcsolódott végpontról milyen egyszerű kódolatlan formában keringő jelszavakat megszerezni.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Közleményünkben szintetizálni kívántuk azon ismeretanyagot, amelyet tanulmányaink, illetőleg kutatásaink során a támadás témakörében eddig elsajátítottunk. Ahogyan azt megfogalmaztuk, a támadáshoz szükséges tudás megszerzése általában hosszú évek kitartó munkája, a rendszerek működésének legmélyebb szintű ismeretével és nagyfokú programozási gyakorlattal társul. A támadási tevékenység kulcsa mégis a támadási képesség megszerzése. Értelmezhető olyan plusz információként, mely birtokában már végrehajtható a támadás.

Anyagunk elméleti síkon és gyakorlati példákon keresztül közelítette meg a témakört, egyúttal reméljük, hogy mindez hasznosíthatóvá válik a szakmai berkekben.

FELHASZNÁLT IRODALOM

[1] Kevin D. Mitnick : A megtévesztés művészete; Perfact-Pro Kft., 2006

[2] Póserné Oláh Valéria : SZÁMÍTÓGÉP-HÁLÓZATI TÁMADÁSOK, Forrás: http://hadmernok.hu/kulonszamok/robothadviseles6/poserne_rw6.html (Letöltve: 2010.03.16)

[3] Krasznay Csaba : A rendszer próbája: az etikus hackelés és penetrációs tesztelés, Forrás: http://www.krasznay.hu/presentation/ethical_hacking_krasznay.ppt (Letöltve: 2010.03.16)

[4] Krasznay Csaba : Információbiztonság a másik oldalról: hackerek Magyarországon – Networkshop 2008 konferencia, Forrás: http://video.google.com/videoplay?docid=4403380718693727650# (Letöltve: 2010.03.16)

13 http://hu.wikipedia.org/wiki/Brute_force-támadás

[5] Buherátor : Mindent az SQL Injection-rol - Hacktivity 2008, Forrás: http://video.google.com/videoplay?docid=1435346511927087441&hl=en# (Letöltve: 2010.03.16)

[6] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal)

[7] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal)

[8] Négyesi Imre: Az információgyűjtés jövőképe (Hadtudományi szemle on-line, I. évfolyam (2008) 3. szám, 95-100. oldal)

[9] Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője (MK KBH Szakmai Szemle 2009. 3. szám, 35-50. oldal, ISSN 1785-1181)

[10] Négyesi Imre: Az önkormányzatok informatikai stratégiája és a Magyar Információs Társadalom Stratégia összefüggései (Hadtudományi szemle on-line, II. évfolyam (2009) 2. szám, 85-92. oldal HU ISSN 2060-0437)

[11] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia előadás, 2010.03.05.-06.)

[12] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05.-06.)

Masenkó-Mavi Viktor – Szalontai László
viktor.masenko@uni-corvinus.hu – laszlo.szalontai@uni-corvinus.hu

A NANOTECHNOLÓGIAI FORRADALOM KIHÍVÁSAI

Absztrakt

Ez a cikk a nanotechnológia alapjairól, fejlődéséről és etikai kérdéseiről nyújt összefoglalást.

This article describes the principles and the evolution of the nanotechnology together with its matter of ethics.

Kulcsszavak: *nanotechnológia ~ nanotechnology*

A nanotechnológiával az emberiség talán egyik legnagyobb kalandja kezdődik el. Mi lesz a kaland vége?- egyelőre senki sem tudja megmondani. Még az űrhajózás kalandjánál is nagyobb kaland elé nézünk, amikor a nanotechnológia révén megkíséreljük feltárni és megérteni a bennünket közvetlenül körülvevő anyag eddig láthatatlan rejtelmeit, törvényszerűségeit. Ezen anyagi világ egy olyan univerzum, amelynek titkai bizonyos mértékig meghaladják a csillagközi, bolygóközi utazás rejtelmeit, a világegyetem megismerésének kihívásait. Az ember mindeddig úgy ahogy eligazodott a mikro, a mezo és a makro világban , de a nano világ egy újszerű, eddig csak felületesen ismert- esetenként csak sejtett- világot tár fel az ember előtt. A nanoszintű ismeretek kiszélesítése ígéretes távlatokat nyít az emberiség előtt, lehetővé válhat nagyon sok függő probléma megoldása.

A nanotechnológia és a nanotudományok napjaink tudományainak egyik legígéretesebb és legdivatosabb ágazata. Az un „nano-őrület" már több évtizede tartja izgalomban a tudósokat és a nagyközönséget. A szóban forgó tudományterület elméleti megalapozása 1959-ben történt meg, amikor Richard Feynmann a kaliforniai műszaki egyetemen megtarotta nagy visszhangot kiváltó előadását[1], amelyben nem tartotta lehetetlennek az atomokon alapuló anyagmérnökséget. Bár itt célszerű felhívni a figyelmet arra, hogy Feynmann, - aki zseniális fizikus volt, kutatói-oktatói tevékenységét Nobel díjjal honorálták - véletlenül keveredett a nanotechnológiai tudomány alapító atyái közé. A nanotechnológiával foglalkozó minden mai tudós illőnek tartja Feynmannra hivatkozni, aki egyébként nem tekinthető a nanotudományok és a nanotechnológia részletes kidolgozójának. A nanotechnológia részletekbe menő kifejtését elsősorban Eric Drexler valósította meg. , aki egy mérnöki végzettségű szakember volt (tanulmányait a MIT-en és a Kaliforniai egyetemen végezte). Annak ellenére, hogy Drexler nagyon sokat tett a nanotechnológia elméleti megalapozása, széleskörű népszerűsítése érdekében (tanulmányok tucatját és több könyvet is publikált, sőt 1986-ban a feleségével együtt létrehozta a Foresight elnevezésű tudományos intézetet)[2], őt nem tekintették elegendő legitimációval rendelkező szakembernek: csak egy egyszerű, túlzásokba eső, fantáziáló mérnökként kezelték. Ezért vált szükségessé Feynmann tekintélyére való hivatkozás. Drexler a nanotechnológia és a nanotudományok igazi

1 Ld. Feynmann: There is a plenty of room at the bottom.- www. caltech.edu/Feynmann/plenty, html
2 Amely Intézet célkitűzéseként szerepelt a társadalom időben történő felkészítése a nanotechnológiai forradalomra.

vizionáriusa volt. Első könyvének[3] köszönhetően (amely több világnyelvén is megjelent), a tágabb értelemben vett nagyközönség először szerezhetett tudomást a nano-világ rejtelmeiről és megértésének lehetséges pozitív valamint negatív következményeiről. Ez a kiadvány igen közérthetően foglalja össze a nanotechnológia lényegét, egyes megállapításai a tudományos-fantasztikum határát súrolják, amelyek nagyon sok, máig tartó, vitát gerjesztettek. A második könyvének[4] már nem volt ekkora visszhangja, mivel abban a szerző a nanotudomány és a nanotechnológia igazi tudományos megalapozottságát, kísérelte meg felvázolni (azt elsősorban a tudományos szakmai közönségnek szánta, ezért annak megértése már sokkal bonyolultabb feladat, a könyv igen sok tudományos egyenletet, kvantumfizikai számítást, bonyolult ábrákat tartalmaz)[5].

A nanotechnológia a gyakorlati megvalósulás szintjét végül 1981-ben érte el, amikor feltalálták a pásztázó alagút-mikroszkópot, amely lehetővé tette a tudósok számára, hogy először és közvetlenül megfigyeljék az anyagok atomisztikus összetételét, illetve, hogy manipulálják az atomokat[6]. Ezen eredmény következményeként1985-ben felfedezték a fullerént, a nanogömböcskéket (bucky ball),majd pedig 1991-ben a szén nanocsövecskéket. Azaz a 80-as, 90-es években a nanotudománynak már kézzelfogható eredményei is voltak, s napjainkban már több mint 600 fogyasztói termék tartalmaz nanoelemeket.

A nanotudományt és a nanotechnológiát ma még sokan a tudományos-fantasztikus irodalom világához tartozó kuriózumként, egyfajta ezoterikus tudományterületként fogják fel. Ebben van is valamiféle részigazság, mivel azok még gyerekcipőben járnak. A nanotechnológiáról egyelőre csak fenntartásokkal lehet beszélni, az még csak a kezdeti lépéseit teszi, fejlődésének első fázisában vagyunk. A következő fejlődési szakaszok még a távoli jövő kérdése. Ezért célszerű jelenleg a nanotudományról és a nano technológiáról együttesen beszélni. Azonban nem kérdéses, hogy fokozatosan, lopakodó módon egyre növekszik térhódítása. A nanotechnológia elemei fellelhetők a modern iparágak legfontosabbjaiban, éspedig: az elektronikában, a vegyiparban, a gyógyszeriparban, a közlekedésben, az élelmiszeriparban.

Sem a nanotudománynak, sem a nanotechnológiának nincs egységes precíz fogalma, azonban mindkét fogalom hátterében kimutatható egy közös, egységesen értelmezett tényező, nevezetesen: az 1 nanométertől 100 nanométerig terjedő mérettartomány. Ezen mérettartományból kiindulva, a nanotudomány az a tudomány, amely az anyagok magatartásával, tulajdonságaiknak vizsgálatával foglalkozik nanoszinten. A nanotechnológia pedig az anyagok nanoszintű elemeinek megtervezésével, előállításával, hasznosításával foglalkozik[7].

A fenti megfogalmazásból pusztán az derül ki, hogy mind a nanotudomány, mind a nanotechnológia. az anyagok sajátosságait, tulajdonságait egy specifikus mérettartományban vizsgálja, ellenőrzi. A mérettartománynak különlegesen fontos, úgy is lehet mondani, meghatározó szerepe van. A nano kifejezés a görög nyelvből származik, s az törpét jelent. Azaz a nanotechnológiát nevezhetnénk törpe technológiának is, értelmezhetnénk a miniatürizálás egyik legújabb jelenségeként. Ez azonban nem lenne helyes, mert nem

3 Ld. Eric Drexler: Engines of creation: The coming era of nanotechnology. New York, Anchor Press 1986. A kiadvány online változatát ld. ericdrexler.com./publications.

4 Ld. Eric Drexler: Nanosystems: molecular machinary, manufacturing and computation. John Wilay and Sons, New York, 1992.- - a kiadvány online változatát ld. ericdrexler.com/publications.

5 Nem szabad figyelmen kívül hagyni azt a tényt, hogy ezen könyve megírásakor Drexler a PhD-jén dolgozott a MIT-en. .A PhD megszerzésével bizonyítani akarta a tudományos establishmentnek, hogy ő nem egyszerűen egy álmodozó, fantáziáló mérnökember. Ez végül is sikerült neki: a MIT-en ő volt az első kutató, aki tudományos fokozatot szerzet t(1991-ben) a molekuláris nanotechnológia terén.

6 Az alagút-mikroszkóp működésének elveiről ld. részletesebben Bíró László Péter: Nanotechnológia (Bevezetö gondolatok a nanotechnológiáról, 2002.12-20.)- www. mta.kfki./hu/int=nano/magyarul/nanotechnológia. html

7 A fenti fogalmi meghatározásokat ld. ilyen értelemben: The Royal Society Report „Nanoscience and nanotechnologies: opportunities and uncertaintes. 2004. p.1-2.

egyszerűen miniatürizálásról van szó, a „nano” annál sokkal többet feltételez: az anyag jellemzőinek nagyon nagy mélységű és összefüggéseiben igen bonyolult ismeretét.
A nanotudomány és a nanotechnológia az anyagok igen piciny, parányi mérettartományába eső részeinek vizsgálatát, ellenőrzését és hasznosítását feltételezi. Azaz a nanotechnológia egyelőre nem valamiféle konkrét tárgyat, kézzelfogható technikai-műszaki szerkezetet jelent, hanem mérettartományt. Amikor 1 nanométerről beszélünk, akkor ténylegesen olyan piciny dologra gondoljunk, amelyet nem csak szabad szemmel, de a hagyományos nagyítókkal, mikroszkóppal sem láthatunk. Ezek a mérhetetlenül parányi részecskék az atomok és a molekulák szintjén helyezkednek el. A nano anyagrészecskék méretének meghatározásával a nanometrológia foglalkozik. Ez is egy fejlődő és kialakulóban lévő tudományterület. A nanometrológia értelmében 1 nanométer a méter egymilliárdod része. Ez a kijelentés, nagyon absztrakt ahhoz, hogy képet alkossunk a nanométer valódi méretéről, parányiságáról. Ezért az alábbiakban ahhoz, hogy az utóbbiról legyen valamiféle elképzelésünk, összehasonlításunk, tájékoztatásul feltüntetünk egy pár egyéb dolog mérettartományát. Így például:

- egy mikron = 1000 nanométer;
- 1 atom = 0.1, 0.5 nanométer (azaz az atomok mérete kisebb a nanométernél);
- 1 A/4-es papírlap vastagsága = 100,000 nanométer;
- 1 vörös vérsejt = 7,000 nanométer;
- 1 nanométer a milliméter egymilliomod része;
- a DNS molekula átmérője = 2-2,5 nanométer;
- 1 tipikus fehérje (pl. a hemoglobin) = 5 nanométer;
- 1 emberi hajszál átmérője = 80,000 nanométer;
- 1 vírus átmérője = 100-150 nanométer;
- 1 légy = 1 millió nanométer;
- 1 nanométer 1 milliószor kisebb, mint egy homokszem;
- és végül tegyünk pontot az „i”re; egy pont az „i” betűn elegendő ahhoz, hogy azon 1 millió nanorészecskét helyezzünk el.

Az 1 től 100-ig terjedő nanométeres tartományhoz való ragaszkodás a nanotudományok terén nem valamiféle megmagyarázhatatlan szeszély. Például a mikront, millimétert, centimétert is technológiai mérceként lehetne használni, de annak nem lenne semmiféle értelme. Nem sok racionalitása lenne millimétertechnológiáról vagy centiméter technológiáról elmélkedni, mint önálló tudományos területről. A nanoszintű mérettartományhoz valamiféle olyan plusz társul, ami szükségessé teszi annak önálló tudományos-technológiai vizsgálatát. Ez a plusz abból adódik, hogy az anyagok tulajdonságai nanoszinten (100 nanométerig bezárólag) jelentősen megváltoznak. A változást két tényező idézi elő: 1) nanoszinten az anyagok 1 tömegegységre jutó fajlagos felülete rendkívül nagy, azaz tényleges felületük jelentősen megnövekszik. Ennek következtében változik (növekszik) az anyag reakcióképessége; 2) nanoszinten az anyagok tulajdonságai tekintetében az un. kvantumhatások lépnek életbe és megszűnnek a hagyományos fizika törvényei. Ezek a hatások változást okoznak az anyag optikai, mágneses, elektromos tulajdonságaiban. Mindez új távlatokat nyit az anyagmérnökség terén, a rendelkezésre álló anyagokból új hasznos tulajdonságokat mutató elemeket, rendszereket lehet létrehozni. Így például a szén nanocsövecskék, amit a modern nanotechnológia egyik legfontosabb vívmányának (csoda-termékének) tekintenek, az alábbi újszerű tulajdonságokat mutatnak fel:

- Szilárdsága: 4.5 milliárd pascal, míg az acél szilárdsága 2 milliárd pascal;
- Áramvezetői képessége: 1 milliárd amper/cm^2, a jelenlegi rézhuzaloké 1 millió amper/cm^2;

- Hővezetői tulajdonsága: 6.000 watt/m/kelvin/szobai hőmérsékleten, míg a tiszta gyémánté 3.320/watt/m/kelvin/szobai hőmérsékleten.

A Drexler által vizionált nanotechnológiai forradalom egyelőre még nem valósult meg. Az atomonkénti építkezésnek(alulról fölfelé történő építkezés)csak részeredményei vannak. Drexler volt az, aki úgy vélte, hogy távlatilag kifejlődhet az atomok és molekulák szintjén történő anyagmérnökség automatizált, előre programozott széleskörű elterjedése. Ehhez azonban túl kell lépni a pásztázó alagút-mikroszkóp által megvalósítható atomisztikus építkezés keretein. Az atomok tervezett összerakásán alapuló mérnökség feltételezi az atomok millióinak, milliárdjainak gyors mozgatását, célzott összerakását., ami valamiféle nano-méretű összeszerelő robot-rendszer kifejlesztését igényli. A Drexleri vízió szerint a jövőben lehetővé válik a nano-robotok (nanobots, nanits) millióinak egyidejű alkalmazására, amelyek képesek lesznek az ember számára hasznos, háromdimenziós termékek előállítására (ezek az összeszerelő robotok: assemblers). Az összeszerelő robotokon kívül működhetnek un. szétszerelő nano-robotok is (disassemblers), amelyek az anyagot molekulákra, atomokra lebontva szedik szét .Továbbá, ezek a robotok képesek lesznek az önsokszorozódásra is (self-replication) Ezen összeszerelő és szétszerelő, illetve önsokszorozódásra képes nano-robotrendszer gyakorlati megvalósíthatósága kapcsán éles viták alakultak ki a különböző tudományágazatok képviselői között. Egyesek kifejezetten elutasítják, fikailag képtelennek tartják az ilyen robotok mechanikailag történő előállítását (azaz az ilyen ” mechanikai mérnökség „kivitelezését nano szinten puszta képzelgésnek tartják). Mások ennek lehetőségét nem zárják ki, példaként a természetben, molekulák és sejtek szintjén végbemenő, évezredek során létező nano-szintű folyamatokra hivatkoznak. Ezen eltérő felfogások alapján alakulhatott ki a száraz (mechanikus) és a nedves (biológiai) nanotechnológia közötti különbségtétel.

A nanotechnológia a 21-22. századok új technológiája, térhódítása a következő évtizedekben igen jelentős hatással lesz életünk minden területén. A nanotechnológia diszruptív, felruházó és interdiszciplináris technológia. Diszruptív azért, mert képes felváltani, megsemmisíteni minden eddigi technológiát, létrehozza a termékek és termelési eljárások új nemzedékét, amelyek a korábbi termékeket és eljárásokat teljesen elavulttá tehetnek. Felruházó technológia azért, mert ugyan úgy, ahogyan a villamos energia, a belső égésű motorok vagy az Internet, amelyek képesek voltak megváltoztatni korábbi életformánkat, a nanotechnológia is társadalmunkat új, sok tekintetben egyelőre még megjósolhatatlan módon, képes átformálni. Interdiszciplináris technológia azért, mert hatása a különböző tudományterületek fokozatos összefonódása révén válik észlelhetővé, csak a különböző tudományterületeken dolgozó tudósok - mint például, biológia, kémia, anyagtudományok, orvostudomány, környezeti tudományok - közös és összehangolt tevékenysége vezethet el a nanotechnológia forradalmához. Ez a forradalom csak nagy nehézségek és igen sok bizonytalanság közepette fog megvalósulni. Erre utal az a tény, hogy már jelenleg is kialakult a nano-optimisták és a nano-pesszimisták tábora. Az optimisták egy olyan új világot vizionálnak melyben a termékek és szolgáltatások költségei radikálisan csökkenek, amelyben a számítógépek teljesítőképessége, működésük gyorsasága több milliószoros lesz a jelenlegi számítógépeknél, s ennek következményeként lehetővé válik az előre programozott termékgyártás, amelyben az orvosi ellátás és gyakorlat terén bevezethető megoldások igen radikális eredményt produkálhatnak, éspedig: a betegségeket véglegesen fel lehet számolni, az öregedést új keretek közé lehet helyezni az élettartam jelentős meghosszabbítása révén, a rokkantság által okozott hátrányos helyzetet fel lehet számolni. A pesszimisták a fentieknél sokkal sötétebben látják a dolgot. Egyesek az aránytalanságok növekedését, az egyenlőség végletes megbomlását vélik felfedezni az új technológia bevezetése folytán. Mások az önsokszorozódásra képes nano-robotok elterjedésének a rémével riogatnak. De vannak olyanok is, akik környezeti katasztrófát jósolnak a

mesterséges nanorészecskék rohamos elterjedése folytán, vagy esetleg globális ökológiai megsemmisülést az ámokfutásba kezdő nano-robotok következtében.

A fenti ellentmondások ellenére, napjainkban a válasz arra a kérdésre, hogy „a nanotechnológia tudomány-e avagy csak tudományos fikció?", csak az lehet, hogy ez a technológia fejlődésének első szakaszába lépett, a modern tudományos és technológiai fejlődés önálló területét alkotja. Azaz a tudományos fikció területéről áttért a valódi, igazi tudomány területére. Még akkor is, ha jelenleg csak gyerekcipőben jár, mivel egyelőre még nem beszélhetünk a nanotechnológia ötletét felkaroló alapító atyák (Feynmann és Drexler) nanovilágáról, de egyértelműen hibás következtetés lenne az a feltevés, amely a nanotechnológiát továbbra is kuriózumként fogná fel. A nanotudományok és a nanotechnológia fejlődése lopakodó módon történik. Egyre növekszik azon termékek száma, amelyek nanotechnológia által előállított elemeket tartalmaznak[8]. 2005-ben a nanotechnológiát tartalmazó termékek összértéke 32 millió dollárt tett ki, becslések szerint 2015-ben ezen érték nagysága elérheti a 3,1 trillió dollárt[9]. Továbbá, a tudományos fikció tézisét cáfolja az is, hogy a nanotudományok és nanotechnológia fejlesztésére az államok milliárdokat (éspedig, dollár- milliárdokat) költenek: 2007-ben a világon összességében 13,8 milliárd dollárt fordítottak az államok a nanotechnológiára[10]. A nanotudományok és a nanotechnológia kutatása és fejlesztése terén az egyes fejlődő országok is (pl. Brazília, Kína, India) fokozatosan felzárkóznak a fejlett országokhoz. Így különösen aktív vonatkozó tevékenységet mutat Kína: a nanotechnológiai szabadalmaztatás terén Kína az USA és Japán mögött a harmadik helyet foglalja el, a kínai Zushou városban nemzetközi nanotechnológiai innovációs parkot létesítettek, amely 14 nanotechnológiában érdekelt vállalat beindításában segédkezett[11]. Az USA-ban a nanotechnológiai kutatásokra szánt állami támogatás mértéke éves szinten megközelítette az 1 milliárd dollárt, ami arra utal, hogy az űrkutatás támogatásán kívül (az Appollo Holdra juttatásának elősegítése), egy bizonyos tudományterület fejlesztésére még soha nem fordítottak ekkora nagyságú állami támogatást[12]. A nanotechnológiai kutatási és fejlesztési programok látványos fejlődéséről az egész világon ld.: Meridian Intézet 2005. évi jelentését[13].

A nanotechnológia tudományos megalapozottságát és a sci-fi határát meghaladó jellegét bizonyítja az a tény is, hogy nemzeti szinten egyre komolyabban és átfogóbban foglalkoznak vele(nemzeti törvényeket, külön főhatóságokat hoznak létre). Ezt az utóbbi folyamatot elsősorban az USA gyakorlata mozdította elő: 2001-ben az USA-ban szövetségi szinten kidolgozták és elfogadták a Nemzet Nanotechnológiai Kezdeményezés Programját (National Nanotechnology Initiative), majd 2003-ban Clinton elnök kezdeményezésére elfogadták a 21. századra szóló Nanotechnológiai Kutatási és Fejlesztési Törvényt (the 21st Century Nanotechnology Research and Development Act -2003). Az amerikai gyakorlat hatására napjainkban kb. 35 országban nemzeti nanotechnológiai kezdeményezési programokat fogadtak el[14].

A kutatási- és fejlesztési programok elterjedésén kívül a nanotechnológia tudományos legitimálását, elszakadását a tudományos-fantasztikum világától bizonyítja az a tény is, hogy

8 Becslések szerint ma már 600-nál is több ilyen termék van forgalomban.
9 Ld.Carole Jacques: Overhyped technology starts to reach potential: nanotech to impact $3.1 trillion in manufactured goods in 2015.- www. carole. jacques@luxresearch.com
10 Ld. Nations worlwide pour billions into nanotechnology.- www. america.gov/st/econ.-English/2008 September/2008092.
11 Ld. ibid.
12 A fenti összehasonlító megállapítást ld. A tiny premier on nano-scale technologies and „the little bang theory". ETC group, June 2005,- www.etcgroup.org
13 ld. Meridian Institute: Nanotechnology and the poor. Opportunities and risks. Closing the gaps, January 2005. p.3-4.- www. meridian- nano.org
14 Ld. M.C. Rocco: Broader societal issues of nanotechnology.- Journal of nanoparticle research, vol .5 2003 p.182.

rangos nemzeti tudományos testületek is napirendre tűzték a nanotechnológia jövőbeni fejlődésének és lehetséges következményeinek a vizsgálatát. Itt talán elegendő három nagy visszhangot kiváltó nemzeti jelentést megemlíteni, éspedig: 1) The Royal Society and the Royal Academy of Engineers: "Nanoscience and nanotechnologies- opportunities and uncertaintees"(2004, London)[15]; 2) The Royal Commission on Environmental Pollution: „Novel materials in the environment- the case of nanotechnology"(2008)[16]; 3) A vonatkozó irányadó jelentések közt kell végezetül megemlíteni a Tudomány és a Technológia kanadai Etikai Bizottságának a nanotechnológia etikájáról szóló 2006. évi jelentését[17].

A nanotudományok és a nanotechnológia elszigeteltsége és komolytalansága ellen hat az a tényező is, hogy tekintélyes nemzetközi kormányközi szervezetek is napirendjükre tűzték ezen tudományok és technológiák kérdéseit, s egyre nagyobb érdeklődést tanúsítanak az említett kérdések iránt. Példaként három nagyobb nemzetközi szervezetet lehet megemlíteni, éspedig: az UNESCO-t, az OECD-t, illetve az Európai Uniót. Amennyiben egy teljesen elvont, pusztán elméleti jelentőségű és ezoterikus tudományról lenne szó, úgy nem igen képzelhető el, hogy ezek a nagyhatalmú- és befolyású szervezetek aktívan bekapcsolódnának a vonatkozó tudományos elemzésekbe.

Az UNESCO keretein belül a nanotechnológiával komolyabban 2003-tól foglalkoznak, amikor is a COMEST 2003 Decemberében a Rio de Janeiro-i ülésén napirendre tűzte ezen technológia kérdéseit. 2005-ben egy külön szakértői csoportot hoztak létre a COMEST égisze alatt, amely feladatul kapta a Szervezetnek a nanotechnológia iránt tanúsított politikájának a kidolgozására[18]. Majd ezen szakértői csoport tagjai 2006-ban egy külön kiadványban foglalták össze megállapításaikat[19].

Ezen kívül, feltétlenül meg kell említeni az Európai Unió egyre növekvő érdeklődését a nanotudományok és a nanotechnológia iránt. Ezt az érdeklődést az alábbi, az Unió égisze alatt elfogadott okmányok támasztják alá:

1) 2004-ben az Európai Bizottság jelentést készített az „Európai nanotechnológiai stratégiáról", amelyben külön kiemelte az európai versenyképesség megőrzésének, illetve a nanotechnológia felelősségteljes fejlesztésének a szükségességét[20];

2) 2005-ben a Bizottság külön jelentésben foglalta össze az európai „Nanotechnológiai Akciótervet", amely tervben a nanotudományok fejlesztésének átfogó és koherens követelményeit, illetve a nanotechnológiai fejlesztési prioritásokat foglalta össze[21];

3) 2007-ben a Tudomány és az Új Technológiák etikai kérdéseivel foglalkozó Európai Munkacsoport (angol elnevezése: European Group on ethics in science and new technologies – EGE) véleményt fogalmazott meg a „nanotechnológia etikai kérdéseiről"[22];

15-Ld. www. raeng. org.uk/news/publications/reports/nanoscience.
16 Ld. rcep.org.uk/27th report/novel%20materials/documents
17 Ld. Commission de l'éthique de la Science et de la Technologie. Position statement: Ethics and nanotechnology.A basis for action.Gouvernment du Québec, 2006.
18 A fenti információkat ld. www. portal.unesco.org/shs/en/ex.php-URL- /ID=6314
19 UNESCO brochure: „The ethics and politics of nanotechnology"- www.portal.unesco.org/shs/en/ex.php-URL-ID=96483 URL
20 Ld. European Commission Communication: „Towards a European Strategy for Nanotechnology", [Com(2004) 338, 12.5.2004].
21 Ld. European Commission: „Nanotechnologies Action Plan"[Com(2005) 243, 7.6.2005]
22 Ld. EGE opinion No.21, 17 January, 2007.

4) És végül az Európai Bizottság 2008-ban egy külön ajánlásban közzé tette a nanotudományok és a nanotechnológiák felelősségteljes kutatásával kapcsolatos magatartás-kódexet[23]. A magatartás-kódex jelentősége, annak ellenére, hogy az jogilag nem kötelező, (az abban foglaltak önkéntes alapon vállalhatók, sőt azoktól el is lehet térni - a szigorúbb szabályozás irányába - mivel a kódex rendelkezései csupán kiegészítik a hatályban lévő szabályozást) igen nagy, hiszen ez az első európai, normatív, precízen rendszerezett, rendelkezéseket tartalmazó, okmány a felelősségteljes nanotechnológiai kutatásról és fejlesztésről. A kódex 7 általános vonatkozó elvet rögzít, éspedig:

a) Fogalmi követelmények (3.1 cikk): a nanotechnológiai kutatásokat a nagyközönség számára is érthető módon kell megvalósítani. Azok során bisztosítani kell az alapjogok védelmét, a kutatások eredményei az egyének és az egész társadalom jólét kell szolgálniuk;

b) Fenntarthatóság (3.2 cikk): a nanotechnológiával kapcsolatos kutatásokat biztonságosan, etikusan, a fenntartható fejlődést is szem előtt tartva, kell megvalósítani. Azok nem keletkeztethetnek vagy okozhatnak biológiai, fizikai vagy erkölcsi kárt vagy veszélyt az emberek, az állatok, a növények és a környezet tekintetében, sem most, sem a jövőben;

c) Elővigyázatosság (3.3 cikk): Ezeket a kutatásokat az elővigyázatosság elvével összhangban kell megvalósítani. Az elővigyázatosság arányosan viszonyul a védelem azon szintjéhez, amely biztosítja a társadalom jólétét szolgáló és a környezetet védő fejlődés előmozdítását;

d) Általános befogadókészség (3.4 cikk): A vonatkozó tudományos kutatásoknak nyitottnak és átláthatónak kell lenniük minden érintett számára (az érintettek teljes köre ide értendő: a kutatásokat végzők, a kutatások eredménye által érintettek). A kutatások transzparenciája magába foglalja az információkhoz való hozzáférés jogát, valamint az érintettek részvételét a döntéshozatali folyamatokban;

e) Kiválósági követelmények (3.5 cikk): A vonatkozó kutatási tevékenységnek összhangban kell lennie a legmagasabb tudományos szabványokkal avégett, hogy biztosítva legyen a kutatás integritása és a helyes laboratóriumi gyakorlat;

f) Innováció (3.6 cikk): A kutatói tevékenységnek ösztönöznie kell az alkotókészség, a rugalmasság, a tervezés maximális megvalósíthatóságát;

g) Felelősség (3.6 cikk): A kutatókat és a kutatói szervezeteket felelőssé kell tenni kutatásaik társadalmi, környezetvédelmi és az emberi egészségre gyakorolt következményeiért, függetlenül attól, hogy ezen következmények a jelenlegi vagy a jövő nemzedékek élete során következnek be.

A kódex a fentieken kívül egy sor általános irányelvet is rögzít, amelyeknek egy része a fentiekben ismertetett általános elveket tovább pontosítja.

23 European Commission: Recommendation of 07/02/2008 on a Code of Conduct for responsible nanosciencies and nanotechnologies research. -[Com(2008) 424 final.

A nanotechnológia rohamos fejlődését, közeli komoly kihívásait támasztja alá az a tény is, hogy azzal egyre gyakrabban foglalkoznak nagy tekintélyű nem-kormányközi nemzetközi szervezetek is. Így például a Kanadában bejegyzett nemzetközi szervezet, az ETC-group[24], igen alapos tanulmányokban és jelentésekben foglalkozik ezen technológia fejlődésének és alkalmazásának következményeivel[25]. A Greenpeace nemzetközi nem-kormányközi szervezet sem maradt tétlenül[26].

A nanotechnológia etikai kérdései

A nanotechnológia tényleges társadalmi következményeinek autentikus felmérése még várat magára - ez nem a véletlen műve, hiszen ma még senki sem képes pontosan megjósolni azt, hogy egy évtized múlva hogyan fog kinézni ez a technológia - bár az is igaz, hogy az egyre szélesedő nanotechnológiai kutatások és kezdeményezések fényében elkezdődött az ilyen értelmű következmények fokozatos feltérképezése is. Az USA-ban a vonatkozó szakirodalom ezen következményekkel kapcsolatos kutatásokat a SEI (social and ethical implications - társadalmi és etikai következmények) vagy az EHS (Environment, health, and safety - környezet, egészség és biztonság) rövidítés által jelölik. Tekintettel arra, hogy a nanotechnológiai forradalom előestéjén vagyunk, az ilyen jellegű felméréseket csak üdvözölni lehet, ámbár ezek a kutatások igen vontatottan haladnak, azokra az egész nanotechnológiát érintő támogatásoknak csak igen kicsiny részét fordítják. A jelenleginél célszerű lenne sokkal nagyobb figyelmet fordítani ezekre a felmérésekre, mivel a nanotechnológia valóban képes radikálisan és kiszámíthatatlanul átformálni jelenlegi életformánkat, forradalmi módon átalakíthatja a bennünket közvetlenül körülvevő világra vonatkozó tudásunkat.

Minden hasznos technológia, ideértve a nanotechnológiát is, komoly és aggasztó etikai kérdéseket vet fel. Megítélésem szerint ezen kérdéseket két nagy csoportra lehet felosztani:

1) általános dilemmák;

2) speciális, csak a nanotechnológiára jellemző kérdések.

Az általános dilemmák közt kell megemlíteni, hogy célszerű-e a társadalomra hirtelen rászabadítani egy ekkora tudással járó hatalmat. Nem kétséges, hogy a nanotechnológia abszolút hatalmat jelent a szervetlen világ fölött, ugyan úgy, ahogyan azt a biotechnológia jelentette a szerves világ fölött, azzal a különbséggel, hogy a nanotechnológia jelentősen növeli az embernek a szerves világ fölötti hatalmát is. Egy ilyen óriási hatalom közkincsé tétele- hiszen a nanotechnológiának csak akkor van igazi értelme, ha azt az emberek a mindennapi életben is felhasználhatják- nem okoz-e végzetes, számunkra egyelőre beláthatatlan és egyúttal megoldhatatlan következményeket?

A nanotechnológia hatalma magában hordozza az emberiség végzetének a lehetőségét is. Ezért egyesek úgy vélik, hogy nem célszerű azt esztelenül forszírozni, jó lenne egy pillanatra megállni a fejlesztés útján és elgondolkodni, s amíg nem tisztázódtak megfelelően a lehetséges problémák, időszerű lenne moratóriumot hirdetni mind a kutatásokra, mind a

24 Az ETC rövidités az Erosion, Technology and Concentration szavakból származik.
25 Ld.1) ETC: The big down: Atomtech technologies converging at the nanoscale, 2003); 2) ETC: Dow non the farm: The impact of nanoscale technologies on food and agriculture; 3) ETC: Nanotech RX-medical applications of nano-scale technologies:what impact on marginalized communities? , 2005.
26 Ld. Alexander Huw Arnall: Future technologies, today's choices. Nanotechnology, artificial intelligence and robotics.- Greenpeace Environmental Trust, London, 2003.

fejlesztésre. Ilyen értelemben foglalt állást Bill Joy, a Sun Microsystem volt vezető programozója, nagy hatást kiváltó tanulmányában" A jövőben miért nincs szükség ránk?"[27]

A másik nagy dilemma a nanotechnológiával való visszaélés lehetősége. A történelmi tapasztalatok fényében minden más technológiával visszaéltek (pl. az egyszerű fémkéstől kezdve - amelyet nem csak az állatok leölésére használtak - az atomenergiáig bezárva - azt nem csak energia előállítás céljára használták fel), a nanotechnológiával is vissza fognak élni, az gonosz és rossz szándékú emberek kezébe kerülhet. De a visszaélés kockázatát elsősorban nem is abban látom, hogy a technológia rossz szándékú emberek birtokába kerül (ezt megakadályozni nem lehet), hanem abban, hogy az adott technológia milyen módon módosíthatja magát az embert, az milyen „hozzáállást" keletkeztet benne. Az igazi kockázat abból adódik, hogy az ember, óriási hatalmának birtokában képtelen lesz ésszerűen dönteni a technológia jó és rossz szándékú felhasználása közötti különbségről. A tudás megszerzésére való törekvés nem öncélúan történik, azt mindig valamilyen tett követi. Arra azonban nincs garancia, hogy a tett csak a jónak az elkövetésére irányul, A tudás nem mindig abból a feltételezésből indul ki, hogy csak jót lehet tenni, hanem abból is, hogy „amit meg lehet tenni, azt meg is kell tenni". A nanotechnológiával sok mindent meglehet tenni, s félő, hogy a megtehetőt meg is fogják tenni. A nanotechnológia intézményesítésével kapcsolatos speciális kérdések közt lehet megemlíteni az alábbiakat:

1) Az un. gray-groo probléma, amit Drexler vetett fel. A gray-grooing lényegében szójáték[28], tartalmát csak körülírással lehet meghatározni, az a nanotechnológiai kutatások jelenlegi szakaszában nem jelentkezik, csak a molekuláris termelés elterjedését követően merülhet fel, s azt az un nano-replikátorok esetleges megjelenésével hozzák összefüggésbe. Azt előre programozott, önsokszorozódásra képes replikátorok egyesek véleménye szerint ámokfutásba kezdhetnek, azaz megtörténhet, hogy a sokszorozódási folyamat nem zárul le, annak nem lesz végső határa, és az egyre sokasodó nanorobotok mindent a saját képükre alakítanak át, a természet minden atomját, molekuláját önmaguk előállítására használják fel, aminek a végeredménye az egész bioszféra megsemmisítése;

2) Annak ellenére, hogy jelenleg még nem beszélhetünk a nanotechnológia forradalmi (a molekuláris termelést is felölelő) szakaszáról, az un. lopakodó, evolúciós nanotechnológia gyakorlati alkalmazása (a jelenleg érvényes technológiák jobbítása, fejlesztése a nanotechnológia révén) egyre szélesebb körben terjed: a nanotechnológiával kapcsolatos „anyagmérnökségnek" látványos eredményei vannak. A nanoméretű anyagok (fullerén, nano széncsövecskék, nano-húzalok, nanogyurmák, különböző fémoxidok, kvantumpöttyök stb.) rohamos léptékű felhasználása már most is komoly etikai kérdéseket vet fel. Elsősorban a fogyasztók szemszögéből. Azért, mert a nanomértékű anyagokat tartalmazó termékeket a gyártók nem látják el külön figyelmeztető címkékkel, s így a fogyasztónak esélye sincs az önvédelemre (még akkor sem, ha felvilágosult a különböző nanorészecskék veszélyeiről). Így például, különösképpen a kozmetikai ipart kell megemlíteni, amelyen belül a kozmetikumoknak (arckrémek, hidratáló szerek, samponok, naptejek) nanorészecskékkel való feldúsítása igen elterjedt. Azaz, egyértelműen a GMO-k felhasználásával kapcsolatos etikátlan gyakorlat megismétlődésének lehetünk a szemtanúi. Ez pedig megingathatja a nanotechnológiába vetett fogyasztói bizalmat.

27 Ld. Bill Joy: Why the Future doesn't need us.-Wired, 8.o4. 1-20pp..- www. wired.com/achive/8.04/joy_ pr.html
28 Talán a Kisgömböcről szóló népmesében szereplő „ham bekaplak"-hoz lehetne leginkább hasonlítani. Drexlert Richard Smallay többször is megrótta a gray-groo probléma felvetése miatt, mivel az csak gyermekek rémisztgetésére jó.

Az élelmiszeripar is gyorsan felismerte a nanotechnológia lehetséges hasznát, s napjainkban rohamosan növekszik az un. nano-élelmiszerek aránya a piaci forgalomban. Az élelmiszeriparban a nanotechnológia honosítása két fő irányra koncentrálódik[29]:

1) Az élelmiszerek új csomagolási technikájának kifejlesztése, amelynek célja az élelmiszerek felhasználhatósági időtartamának növelése, az élelmiszerbiztonság jobbítása, a fogyasztók jobb és pontosabb tájékoztatása a szennyezett és romlott termékek forgalomban történő jelenlétéről. Ezen főirány keretein belül az un. „intelligens csomagolóanyagok" meghonosítása igen nagy szerepet kap. Így például, olyan csomagolási anyagokat lehet alkalmazni, amelyek azonnal jelzik az élelmiszer megromlásának kezdetét, azzal hogy megváltozik a csomagolás színe. A konzervdoboz vagy a műanyag-csomagolás veszélyre (a szavatosság idejének lejárta, a fogyaszthatóság tilalma) figyelmeztető színt vehet fel. Ezen kívül lehetővé válhat a csomagolás önjavító képességének a kifejlesztése is: ha a csomagolás megsérül, akkor az saját magát kijavítja, „befoltozza".Az élelmiszer eltarthatóságának az idejét is növelni lehet azzal, hogy lassítani lehet az oxidálódási folyamatot, semlegesíteni lehet az érést elősegítő gázokat (etilén), s amennyiben elkezdődik a romlási folyamat csomagolás érzékeli a romlással járó enzimeket és automatikusan tartósítószert adagol az élelmiszerhez.

2) A második főirány keretein belül elsősorban az élelmiszereknek jobb, felturbózott hasznosításáról van szó. Ezek közt említhető a forgalomba kerülő élelmiszerek szerkezetének, tápértékének, színének, ízének, illatának minőségi növelése. Különböző nanokapszulákat biológiailag hasznos anyagokkal (vitaminokkal, antioxidánsokkal) vagy esetleg baktériumokat elpusztító szerekkel töltenek meg, amelyek a szervezetbe jutva kiszabadulnak ezen kapszulákból és közvetlenül hasznosulnak. A termékek jobb és esztétikusabb megjelenítése is célként szerepelhet: így például a rostos narancsléket összecsomósodásuk megelőzése, illetve áttetsző színük megőrzése céljából nanorészecskékkel dúsítják. Az ezüst nanorészecskéket, mikrobaölő tulajdonságuk miatt egyre gyakrabban alkalmazzák az élelmiszeriparban. A szén nanocsövecskék pedig egyértelműen megsemmisítik a baktériumokat (pl. sikeresen használták fel azokat az E.coli és a szalmonella baktériumok elpusztítására). Napjainkban az ivóvizet például vasoxid nanorészecskékkel tisztítják, amelyek semlegesítik a szerves szennyeződést és elpusztítják a mikróbákat. Továbbá egyre jobban terjed a különböző nanorészecskéket tartalmazó nanobevonatok alkalmazása, amelyek képesek semlegesíteni a gyümölcsökben és zöldségekben fellelhető vegyszermaradványokat, s hatékony védelmet nyújtanak a különböző patogénekkel szemben. A fentiekből egyértelműen kiderül, hogy a piaci forgalomban lévő nano-termékek száma egyre növekszik, s arányuk a jövőben csak növekedni fog. Etikus-e piacra dobni, engedélyezni a kereskedelmi forgalmát olyan termékeknek, amelyekre nem vonatkoznak speciális szabályozási normák és szabványok?

Az etikusság speciális kérdéseként kell kezelni a nanotechnológia emberi egészségre és környezetre gyakorolt lehetséges hatásainak a vizsgálatát is. Ezen kérdések tisztázatlansága és vonatkozó ismereteink hiányossága, bizonytalansága felveti azt a nagy dilemmát, hogy etikus-e erőltetni az új technológia egyre szélesebb körű alkalmazását a szükséges tudományos bizonyosság kialakulása előtt.

29 Az élelmiszeripari nanotechnológiát ld.: Bhupinder S Sekhon: Food nanotechnology - an overview.- Nanotechnology, Science and Applications, 2010 No.3. Dove Press. pp.1-15.

A mesterségesen előállított nano-részecskék egészségi és természetre gyakorolt hatásairól egyelőre csak nagyon korlátozott ismeretekkel rendelkezünk, mely ismeretek megszerzése egyáltalán nem tűnik egyszerű feladatnak:

- Először is, a különböző méretű nano-részecskék tucatja van forgalomban, az eltérő méretű részecskék pedig eltérő tulajdonságokkal rendelkeznek;
- Másodszor a részecskék sok esetben kompozitok (azaz több összetevőjük van, vagy sajátos bevonatokkal látják el azokat);
- Harmadszor, a méreten kívül a formának is van jelentősége és sajátossága. A különböző formájú nano-részecskék különböző módon viselkednek, eltérő toxicitással vagy más káros hatással rendelkezhetnek. Már bebizonyították, hogy a nagyobb méretű, a hosszú, nano széncsövecskék káros hatása sokkal nagyobb a kisebb méretűeknél;
- Negyedszer,az azonos jellegű nano-részecskéknek az előállításuktól függően lehetnek eltérő tulajdonságai. Például a más-más előállítóktól származó szén nanocsövecskéknek eltérő tulajdonságai lehetnek;
- Ötödször, a nanorészecskék hosszú távú következményeinek, azok egész életciklusára kiterjedő ismeretünk is nagyon hiányos.

Ezen sok bizonytalansági tényező együttes figyelembe vétele már-már megoldhatatlan kihívásnak tűnik. Félő. Hogy egyes tényezők figyelmen kívül hagyása, negligálása a részsikerek fényében a történelem során már tapasztalt egészségi és környezeti problémák váratlan és hatványozott megjelenésével járhat. Például annak idején az azbesztet és a freongázt is csoda-anyagkén könyvelték el, s csak évtizedek múltán jöttek rá arra, hogy azok az egészségre és a környezetre is nagyon káros hatással vannak. De ilyen értelemben példaként említhető a dohányzás is, melynek egészségre káros hatásait csak évszázadok után fedezték fel.

A speciális etikai kérdések közt kell megemlíteni a nanotechnológia szabályozásának jelenlegi hiányát, a vonatkozó szabályozási modellek kidolgozatlanságát. Az államok egyelőre tartózkodnak külön szabályozás beiktatásától, attól tartva, hogy egy szigorú és következetes szabályozás gátja lehet az egész nano-ipar fejlesztésének. Ezért inkább eltekintenek a konkrét szabályozási elvek meghatározásától. Ezen probléma megoldatlanságának etikai aspektusa egyre szembeötlőbb: a piacon forgalomban levő nano-termékek száma egyre növekszik. Etikus-e piacra dobni olyan termékeket, amelyekre nem vonatkoznak speciális szabályozási elvek és szabványok?

A speciális etikai kérdések közt szerepel a nanotechnológiának az emberi képességek megnövelésére, az emberek „jobbítására”, „tökéletesítésére”(human enhancement) valkó felhasználásának kérdése is.

A nanotechnológia etikusságának problémaköréhez tartozónak kell sorolni ezen technológia esetleges katonai felhasználásának a kérdéseit is. Már pusztán azon tény miatt, hogy egyelőre semmiféle nemzetközi megállapodás nem jött létre katonai célú felhasználásáról - továbbá, hogy a jelenleg érvényben lévő fegyverzetkorlátozási megállapodások (atom-, biológiai- és vegyi fegyverek) nem terjednek ki a nanotechnológiára, s azok eleve alkalmatlanok a nano-fegyverek alkalmazásának ellenőrzését illetően - komoly etikai dilemmát vet fel. Megítélésem szerint, a nano-fegyverek kifejlesztésére irányuló erőfeszítéseket mindaddig etikátlannak kell tekinteni, amíg nem alakult ki valamiféle egységes konszenzus katonai alkalmazásának elveiről és normáiról.

A nanotechnológia radikálisan átalakíthatja a hadviselés módját és célját, mindazt, amit a modern hadviselés alatt értünk. Az un. nano-robotok hadrendbe állítása óriási fegyverkezési versenyt indíthat el a nemzetállamok között, aminek következményei beláthatatlanok.

Jelenleg nagyon korlátozott tudással és információkkal rendelkezünk a nanotechnológiával kapcsolatos katonai fejlesztésekről, s a beavatott szakemberek is, ha megkérdezzük őket, milyen jellegű kutatások vannak folyamatban, csak hosszú hallgatás után, szemforgató és értetlenkedő arckifejezéssel válaszolnak. Azaz azon a véleményen vannak, hogy egyelőre jobb is, ha nem tudunk azokról.

A láthatatlan és előre programozott nano-botok alkalmazására (bevetésére) az ellenfél tudomása nélkül kerülhet sor, anélkül, hogy a védekezés bármilyen esélyével rendelkezzék. Természetesen annak van nagy jelentősége, hogy az előre programozás mire terjed ki: annak lehetnek erkölcsileg kifogásolható, aljas szándékú céljai. Például, célként szerepelhet az, hogy az ellenfél állományának tagjaiban molekuláris rendellenességet váltsanak ki. De ezt a programozást sokkal célorientáltabban is el lehet végezni: úgy hogy a nano- botok csak egy bizonyos etnikai vagy faji sajátosságot felmutató egyénekben okozzanak rendellenességet. Azaz lehetővé válhat az előre programozott népirtás is.

A nanotechnológia katonai célú felhasználása nem minden esetben tekinthető ab ovo erkölcsileg kifogásolható célkitűzésnek, Azt nem csak erkölcsileg elítélendő, aljas szándékú támadó fegyverként lehet felhasználni. Célként szerepelhet a megbízhatóbb információgyűjtés, a katonák harci képességének (szellemi és fizikai) javítása, egészségük fokozottabb megőrzése.

A nanotechnológia katonai felhasználásának etikussága közvetlenül összefügg a vonatkozó kutatások és fejlesztések titkosságának tényével[30]. Ezek a fejlesztések hétpecsétes titok alatt folynak, s egyelőre csak azok az elképzelések kerülnek napvilágra, amelyek ezen technológia ártalmatlan (nem gonosz szándékú) felhasználását célozzák. Az azonban, hogy ténylegesen mi zajlik a vonatkozó titkos katonai laboratóriumokban, a közvélemény teljes kizárásával történik.

A nanotechnológia által biztosítható lehetőségek, előnyök igen hamar felkeltette a hadi ipar figyelmét, s ma már terjedelmes katonai kutatásokat végeznek az egyes nemzetállamok (pl. USA, Oroszország, Kína, India). Az USA-ban ismerték fel a legkorábban ezeket a lehetőségeket, s az amerikai hadsereg a Nemzeti Nanotechnológiai Kezdeményezésben már a kezdetektől nagyon aktív szeret vállalt: A DARPA (Defense Advanced Research Projects Agency - A Fejlett Védelmi Kutatások Hivatala)[31] finanszírozza a Kezdeményezés által felölelt programok kb. 40%-át. Ezen kívül az amerikai hadsereg kezdeményezésére és finanszírozása révén az egyik legprominensebb amerikai műszaki egyetemen, a MIT keretein belül, 2002-ben felállításra került egy 50-fős Katonai Nanotechnológiai Intézet (Institute of Soldiers Nanotechnology)[32]. Az Intézet létrehozásában nagy szerepe volt az un. NBIC-jelentéseknek[33], amelyek részletesen tárgyalták a nanotechnológia védelmi célokból történő felhasználásának kérdéseit is. Az eddig napvilágot látott információk szerint a Katonai Nanotechnológiai Intézet elsősorban a katonák jobb és tökéletesebb személyes védelmének jövőbeli infrastruktúrájának kérdéseit vizsgálja és fejleszti. Ezen infrastruktúra központi elemét képezi egy un. könnyített, kényelmes, szuperbiztonságos és intelligens katonai harci uniformis létrehozása.

A harci felszerelésben lévő modern katona logisztikai lábnyoma óriási: a menetkész logisztikai eszközök - fegyverzet, ruházat, kisegítő műszaki eszközök - súlya kb. 65 kg, ami nem pusztán megterhelő a katona szemszögéből, de korlátozza a mozgékonyságát is. Az Intézetben azon dolgoznak, hogy jelentősen csökkentsék a hivatkozott logisztikai lábnyomot, a katona menetkész felszerelésének súlyát 25 kg-ra akarják leszorítani. Az uniformis intelligens módon képes lesz alkalmazkodni a környezethez: az álcázás előmozdítása

30 Ld. ilyen értelemben a Royal Society jelentésének 6.fejezetét, 29.§.
31 A Hivatalt 1958-ban, az első orosz Sputnyik fellövését követően hozták létre.
32 Ld. www.//: MIT/edu./isn.
33 A NBIC-jelentéseket ld. részletesebben: Masenkó-Mavi Viktor: Konvergáló tudományok és technológiák.

céljából automatikusan megváltoztatja a színét, a hőmérséklettől függően vagy melegít, vagy hűt. Továbbá, szükség esetén gyógyítja is a katonát: gyógyszert adagol, vérzést állít el, stb. Sőt, szükség esetén egyes elemei alakváltozásra is képesek lesznek: így például az ingujj több méteres kötöző fáslivá alakulhat, vagy a nadrágszár megmerevedik és átveszi a „sín" szerepét lábtörés esetén.

A nanotechnológia felhasználásával összefüggő etikai kérdések rendszerét, pontos katalógusát jelenleg nem lehet megbízhatóan rögzíteni, mivel ez a technológia az evolúció szakaszában van, s nem lehet előre megjósolni, hogy a jövőben milyen konkrét problémákat vethet fel. Talán ezzel is magyarázható, hogy az egyes kivételektől eltekintve, sem a nemzeti, sem a nemzetközi hatóságok, intézmények nem vállalkoznak egy ilyen katalógus felállítására. A hivatkozott kivételként kell megemlíteni az osztrák Bioetikai Bizottság 2007. évi döntését a „nanotechnológia etikai kérdéseinek katalógusáról"[34].

A Bizottság döntésében nagyon óvatosan - úgy is mondhatnám kissé elnagyolva - közelíti meg a problémát. Elsősorban az orvosi etika és a nano etika összefüggéseit hangsúlyozza. A fentiekben már hivatkozott etikai kérdéseken kívül, az etikusság elemeihez sorolja az alábbiakat:

- a technológia orvosi célból való alkalmazásának kérdéseit;
- az igazságosság problémáját, a szolgáltatásokhoz való általános hozzáférés szemszögéből;
- a magánélet fokozott védelmének szükségességét a nano érában;
- a betegségek diagnosztizálása és azok esetleges gyógyítása közötti szakadék áthidalásának igénye: a nanotechnológia gyors és nagyon pontos diagnosztizálást tesz lehetővé. (Etikailag valóban kérdéses lehet az olyan betegségek diagnosztizálása, amelyeket az adott pillanatban még nem lehet gyógyítani. - M.V.);
- emberi mivoltunk önértékelésének módosulása a nanomedicina fényében, ideértve a betegséghez való viszonyunk változását és a nano-eszközök által megvalósuló állandó önellenőrzés hatását a felelősségtudatunkra.

34 Ld. Bioethics Commission Österreich Ruling of 13 June 2007 „A catalogue of ethical problems and recommendations".- www. Austria, bka.gv. attDoc view.axd/cobld=24586.

Beatrix Fregan
fregan.beatrix@zmne.hu

UN PERSONNAGE ÉMINENT DE L'HISTOIRE DE LA DÉFENSE HONGROISE

Absztrakt

A cikk a felsőfokú nemzeti tisztképzés szerepét mutatja be egy kiemelkedő parancsnok és híradó tiszttársai portréján keresztül a magyar történelem egy nehéz időszakában.

L'article présente le rôle de la formation nationale d'officier supérieur à travers le portrait d'un commandant excellent et de ses camarades transmetteurs dans une période difficile de l'histoire hongroise.

Kulcsszavak: *akadémia, felelősség ~ académie, responsabilité*

Cet article a pour objectif de présenter le colonel András Márton, commandant de l'Académie supérieure militaire hongroise pendant l'insurrection hongroise de 1956.

András Márton, capitaine encore en 1949, est devenu colonel en décembre 1952 à 29 ans à peine. Ce fut une carrière exceptionnelle par rapport à celles de l'époque.

En novembre 1955 le colonel a été nommé commandant adjoint général de l'Académie supérieure militaire Miklós Zrínyi puis commandant le 1e octobre 1956. Cette nomination était évidente pour tout le monde car l'Académie avait besoin d'un nouveau regard pour rafraîchir ses murs anciens. La majorité du corps professoral a accueilli avec sympathie la relève du commandant et a fondé de grandes espérances sur sa personne.

Le crédo militaire du colonel András Márton était alors déjà visible. Il appela à „l'Ordre" ce qui caractérisait tous ses efforts et tous ses consignes pendant la révolution de 1956.

Ses subordonnés ont vite reconnu qu'il assumait toujours la responsabilité de ses hommes ce qui lui a permis de garder la cohésion de l'Académie. Il n'y eut aucune insurrection intérieure ou manifestation extrémiste, bref ses collaborateurs l'écoutaient, à voir la confiance en lui leur donna un certain sens de sécurité.

Deux officiers de Transmissions de l'Académie s'attachèrent étroitement aux activités du commandant. János Haász, chef de transmissions du Passage Corvin devenu un centre important de la résistance, fut l'un de ceux qui étaient affectés dans les rues. Le commandant avait pour ambition de mettre de l'ordre avec ses militaires parmi les „garçons du passage Corvin". Le deuxième officier de Transmissions fut le capitaine Arnóczky, collaborateur proche du commandant de l'Académie.

Le 10 novembre 1956 le colonel András Márton a réuni les officiers de l'Académie pour „leur déclarer qu'à l'Académie il fallait avoir de l'ordre." – a-t-il dit. Après la révolution il avait toujours confiance en la direction militaire du nouveau pouvoir mais il fut vite déçu. Les officiers désirant continuer leur carrière militaire dans l'armée ont du signer une déclaration d'officier. Le colonel Márton l'a également signée mais il ne voulait pas que l'Académie perde sa cohésion. Il a préféré choisir de démissionner puis de prendre sa retraite. Les nouveaux décideurs militaires ont laissé partir un chef de qualité ayant gardé son sang froid aux moments les plus chauds.

Le 5 février 1957 le colonel en réserve András Márton fut arrêté pour son rôle pendant la révolution. Qu'est-ce qu'il a fait? Rien. Il n'a voulu que l'ordre dans les rues. Il a affecté des officiers pour ramener l'ordre et donner des consignes aux insurgés encore à l'âge d'enfance.

Le 9 septembre 1958 la condamnation fut déclarée: 10 ans de prison, rétrogradation, confiscation de biens. Le monde extérieur n'en savait rien.

A l'automne 1960 András Márton, colonel privé de son grade menotté, fut amené de Vác à Budapest au procès du colonel Dienes, son ancien subordonné pour être écouté en tant que témoin.

Arrivant dans le couloir du tribunal il était salué par les officiers de l'Académie cités comme témoin se levant l'un après l'autre pour lui souhaiter avec respect du courage et de la santé.

L'acte d'accusation de András Márton est une lecture à analyser surtout sémantiquement. Elle ressemble énormément à celui créée contre Imre Garab à Debrecen sur le plan linguistique et terminologique. Le lecteur ne peut pas se débarrasser de l'idée qu'elle fut le résultat d'un ordre central. Les accusateurs n'ont pas voulu s'en remettre au hasard. 121 personnes ont été interrogées lors du procès de András Márton.

En avril 1962 la porte de sa prison s'est ouverte et il fut libéré après cinq ans et demi avec amnistie.

Après sa libération plusieurs personnes ont voulu le voir mais il n'a rien accepté des représentants du pouvoir. Les années passées en prison ont forgé sa personnalité. Il a souvent déclaré qu'il n'avait pas envie de se venger et qu'il ne se considérait pas comme un héros, au contraire il refusa ce titre. Il assuma tout ce qu'il avait fait à ce temps-là, y compris les huit points d'accusation, mais il ne se sentait jamais coupable et il ne pourra jamais oublier les choses qui lui sont arrivées.

On a écrit beaucoup de choses sur l'histoire de 1956. Cependant quand on s'intéresse aux événements une question se pose: Comment András Márton s'est-il retrouvé au passage Corvin?

„Justifiez-vous!" András Márton a entendu cette ordre claire et simple dans la rue en se montrant dans la tourelle d'un char T34. La voix venait d'un enfant qu'il n'a pas vu. Au bout d'un certain temps il a vu un petit garçon. Son faux-nom était petit marmot. András Márton lui répondit: „Mon fils, il ne faut pas s'adresser comme ça à un colonel." Finalement le petit marmot monta dans le char et amena le colonel à son chef au passage Corvin.

En entrant dans le cinéma Corvin (poste de commandement des résistants) il a entendu dire:

„Mais qu'est-ce qu'un officier communiste fait là? Tuez-le." Les enfants n'ont heureusement pas tiré puis leur commandant Iván Kovács lança: "on n'accepte pas de conseil d'un communiste." Il y eut une dispute après laquelle les garçons choisirent un nouveau commandant.

Le colonel András Márton a ensuite affecté dix jeunes officiers au passage Corvin que les historiens réussirent à identifier.

András Márton a été le commandant de l'Académie pendant quarante-cinq jours, raison pour laquelle il a subi 1884 jours en prison. Pour chaque jour qu'il a passé en tant commandant de l'Académie il „mérita" quarante-cinq jours dans en prison.

Pendant ce court temps de son commandement les officiers l'ont suivi instinctivement, il l'écoutait toujours. Quelques départements parlaient de sa nomination au poste de ministre.

Il a commandé l'Académie dans une période complexe où la situation changea du jour au lendemain dans les rues. Il savait toujours mener son institut à la baguette. András Márton fut naturellement réhabilité. En tant que général de corps d'armée il répond souvent aux demandes d'invitations. Au centre de son travail social il essaie de conserver le vrai esprit de 1956 en ayant des capacités mentales excellentes.

Il faudra encore beaucoup de temps pour avoir des réponses fiables et objectives aux questions qui demeurent à l'ordre du jour depuis des décennies et surtout depuis la relève du régime et qui sont d'actualité politique quotidienne.

Nous en esquissons quelques unes, dont l'analyse scientifique est en cours.

Voyons qu'au sujet de la demande de pardon qu'est-ce qui pourra s'avérer une solution rassurante?

Une fois la réhabilitation réalisée pourquoi les gens de 1956 sont-ils tout de même déçus?

Du point de vue militaire la question la plus intéressante peut se poser de façon suivante:

Est-ce qu'il y eut une chance? Non, il n'y en eut ni politiquement, ni militairement.

A ce temps-là la politique agressive liée au statut de grande puissance de l'Union Soviétique rendit évident, et non seulement pour les hongrois qu'il n'y avait pas de débouché ou de fuite. Les pays du camp socialiste tombèrent dans leur propre prison eux-même et la force militaire de l'Union Soviétique veillait au maintien du statut quo. L'Occident soutenait les pays socialistes en théorie mais les actions montrèrent autre chose. Le monde occidental trouvait qu'il ne valait pas le coup de prendre des risques pour nous, les Hongrois. Il s'avéra que les dirigeants des Etats-Unies ont même rassuré l'Union Soviétique qu'elle pouvait faire ce qu'elle voulait parce que le système Yalta ne changerait pas. De plus il y avait l'affaire de Suez.

La réaction de l'environnement proche, donc des pays socialistes était fraternelle, du moins des grandes puissances. Les frères de l'Orient lointaine en particulier des chinois se sont exprimés. Le comportement hypocrite de la Yougoslavie pourrait faire l'objet d'une étude spéciale sans parler de la Roumanie „accueillant" le groupe de Imre Nagy. Du point de vue militaire l'armée soviétique stationnait provisoirement dans le pays ce qui a tout expliqué. Dans certains pays amis surtout en Roumanie des divisions soviétiques étaient en réserve avec des unités aériennes aptes au combat. Nous étions entourés d'une force militaire qui aurait pu intervenir contre nous. Tout était prêt à l'échec.

Dans l'armée hongroise il y avait une centaine de militaires qui connaissaient bien la force armée de l'Union Soviétique puisqu'ils y avaient fait leurs études pendant de longues années. Quand on veut soupeser les chances il faut avouer la dure vérité. Nous devons faire la différence entre les insurgés équipés d'un seul fusil appelés garçons de Pest et l'incapacité de prise de décisions des chefs militaires hautement qualifiés. L'enthousiasme des garçons de Pest s'inspirait du manque d'informations et d'organisation militaire dans les situations concrètes car en réalité il s'agissait d'une révolution. L'appréciation d'un commandant disposant de pouvoir se fait sur la base de différentes critères, ce qui peut avoir un point de vue spécial en cas de révolution.

On dit que les Hongrois ne peuvent lutter qu'en cas de supériorité de l'ennemi. Mais il faut reconnaître que le combat contre les soviétiques était désespéré que l'élan sincère des Hongrois n'a pas pu non plus compensé. La période d'après–révolution se caractérise par la rétorsion irrationnelle dont les dimensions ont été révélées bien plus tard et se sont incrustées comme l'une des périodes les plus sombres dans la mémoire des gens.

Zoltán Rajnai
rajnai.zoltan@zmne.hu

DÉVELOPPEMENT DU RÉSEAU TACTIQUE DES FORCES TERRESTRES

Absztrakt

Ez a cikk bemutatja, hogy a védelmi célú harcászati hálózatok milyen szükségletekkel rendelkeznek, és az adatátvitel biztonsága, a hálózatok gyors telepíthetősége milyen jelentőséggel bír.

Cet article présente les besoins opérationnels prioritaires, exprimés par les Forces Armées, l'un des plus importants a été certainement de donner aux moyens de Transmissions une véritable capacité de déploiement et de mise en oeuvre rapide des équipements avec le minimum de personnels.

Kulcsszavak: *hálózatbiztonság, harcászati hálózat telepítése. üzemeltetése ~ sécurisation des réseaux, mise en oeuvre du réseau tactique*

Nous avons une grande ambition a satisfaire l'objectif des Forces Armées Hongroises de disposer de moyens de commandement et de communications opérationnels et conformes avec l'OTAN.

Voyons d'abord les moyens de transmissions qui constituent l'architecture des communications tactiques d'une grande unité opérationnelle:

- au niveau des sections, des compagnies et jusqu'au bataillon les moyens de transmissions sont essentiellement des radios tactiques HF, et VHF dont les dernières générations sont capables de transmettre des données IP entre les systèmes C2 des différents niveaux de commandement:
- à partir du niveau bataillon les postes de commandement sont connectés au réseau maillé soit par Radio de Combat (RFP) soit par Faisceaux Hertziens;
- les Postes de Commandement disposent d'une station et de moyens LAN associés pour offrir des services multimédia aux usagers;
- le système peut bien sûr être connecté au réseau d'infrastructure fixe ainsi qu'aux réseaux de l'OTAN.

Parmi les besoins opérationnels prioritaires, exprimés par les Forces Armées, l'un des plus importants a été certainement de donner aux moyens de Transmissions une véritable capacité de déploiement et de mise en oeuvre rapide des équipements avec le minimum de personnels.

- - Les systèmes de communications tactiques de la génération précédente, et encore en service dans la grande majorité des armées, sont organisés en noeuds de Transmissions de la taille d'une section. Il faut une trentaine d'hommes et une dizaine de véhicules pour assurer la fonction de Centre de Transmissions. Le volume et le poids de ces moyens, les personnels nécessaires à leur mise en oeuvre, sont peu compatibles avec les impératifs de déploiement rapide;

- - L'élément de base autonome a été réduit à un seul véhicule de transmissions et un véhicule cargo pour les antennes et accessoires, servis normelemant par un groupe de 6 personnels: 1 officier - 2 Sous Officiers et 3 opérateurs et conducteurs;
- - Sur le plan économique l'architecture réduit fortement le coût d'acquisition et d'exploitation du réseau tactique:
    - en terme de nombre de véhicules et de stations de transmissions;
    - et pour le nombre de personnels qualifiés nécessaires à sa mise en oeuvre.

Les briques du systéme de télécommunication tactique

Le réseau est un réseau de zone maillé, dont la finalité est de couvrir très rapidement une zone opérationnelle d'artères de communication sécurisées. Il est d'abord constitué de stations de Transit et d'intégration radio. Ces stations seront raccordées entre elles par des Faisceaux Hertziens. Le réseau de Transit permet de raccorder les Stations d'Accés:

- - des Postes de Commandement de Division et de Brigade installés en shelters ou dans des batiments suivant le cas;
- - et des Postes de Commandement de Bataillon installés dans des véhicules de commandement blindés a roue.

Le réseau de Transit permet aussi de raccorder d'une manière totalement automatique les usagers mobiles dotés de postes radio VHF.

Le déploiement sur un site d'une station est grandement facilité par la possibilité d'installer les mâts d'antenne des faisceaux hertziens jusqu'à 600 mètres de la station et raccordés par des cables à fibres optiques. Ainsi en terrain difficile la station peut être camouflée en toute sécurité en bas d'un point haut, alors que les mâts d'antenne seront installés sur la crête militaire autour de ce point haut. Les liaisons de maillage sont réalisées en Bande 4 OTAN, c'est à dire de 4.4 à 5 GHz, avec un débit de 8 Mb/s. Deux antennes peuvent être installées sur un même mât. Les liaisons de raccordement vers les postes de commandement peuvent être effectuées soit en Bande 4 OTAN avec un débit de 8 Mb/s, soit en bande 5 OTAN avec un débit plus important de 34 Mb/s. La station est opérationnelle avec une première liaison hertzienne en fonctionnement dans les 30 minutes après l'arrivée sur le site.

Sur le meme principe qu'une station satellite le PC est constitué d'une partie intérieure et d'une partie extérieure, les deux étant reliés par une fibre optique de 600 mètres.

- l'équipement extérieur comprenant l'antenne et la partie Radio Fréquence (RF) émission et réception intégrée;
- en version Bande 4 (bande des 5 GHz) le PC est constitué d'une antenne électronique de type patch. Le faisceau est formé par la combinaison des multiples patchs émetteurs;
- en version Bande 5 (15 GHz), le PC comprend une antenne parabolique classique;
- l'équipement intérieur dit « Bande de Base » (BBE) est commun quelque soit la bande utilisée pour la liaison. Il se trouve dans la station technique, un même équipement BBE peut être connecté à trois PC et donc permettre trois liaisons.

Cette solution comme nous l'avons vu permet d'éloigner les antennes hertziennes de la station et facilite l'installation et le camouflage sur le site;
- un combiné d'exploitation permet d'assurer d'une part la fonction de chargement des parametres radio de la liaison et d'autre part la fonction de Voie de service entre les opérateurs.

La mise en oeuvre typique d'une station de nouvelle génération avec un Faisceau Hertzien en version Bande IV:

- l'antenne électronique sur son mât en fibre de carbone;
- un touret d'alimentation électrique et de télécommande contenant un UPS (batterie) pour la réalisation immédiate d'une jonction;
- le combiné d'exploitation;
- l'équipement Bande de Base situé dans la station technique;
- un touret de Fibre optique d'une longueur de 600 mètres;
- si la distance avec la station est importante on utilise un petit groupe électrogène pour alimenter l'équipement.

Le détail de l'antenne électronique, qui est dotée d'un système d'alignement automatique de pointage vers la station correspondante. Le FH en Bande 4 permet un débit de 8 Mb/s pour des liaisons d'une portée moyenne radio de 30 à 40 km. Une version en bande 4 offrant un débit de 34 Mb/s est en cours de réalisation pour satisfaire au besoin de plus en plus pressant d'augmentation de débit exprimé par de nombreuses armées.

Typiquement la station en camionnette tactique permet de desservir un poste de commandement d'environ 80 usagers et de raccorder 5 LAN pour les Systèmes d'information Opératiannels et la bureautique. La station du réseau en Véhicule de l'Avant Blindé permet quant à elle de desservir un poste de commandement tactique jusqu'a 40 usagers et de raccorder aussi 5 LAN.

Les usagers mobiles dotés de postes de radio de combat disposent d'un service automatique et sécurisé de radio-téléphone avec des fonctions phonie et transmissions de données. Les radios mobiles peuvent appeler d'autres mobiles ou des usagers fixes du réseau sans l'intermédiaire d'aucun opérateur D'autre part a travers le réseau tactique i1s peuvent joindre les usagers des réseaux d'infrastructure ou des réseaux alliés connectés au réseau.

En cours de déplacement les radios mobiles disposent d'une fonction automatique de changement de balise radio camme dans un réseau cellulaire.

Les fonctions d'administration et de commandement sont assurés par le système de gestion du réseau. Ce système NMS est constitué de deux ensembles, d'une part les stations qui assurent l'administration complète du réseau, et d'autre part les terminaux de gestion locale présents à chaque station du réseau. Une station peut assurer à elle seule le management d'un réseau déployé en opération. Mais dans le cas d'un réseau important les fonctions de planification et de commandement du réseau, de gestion de l'annuaire des usagers, de logistique des noeuds de transmissions peuvent être réparties entre plusieurs stations. Les stations sont alors au nombre de deux ou trois pour un réseau de grande unité, elles sont normalement localisées dans les Postes de Commandement importants.

Les stations constituent un système de gestion et d'administration distribué, où chaque station met à jour en temps réel les autres stations du réseau. Les stations NMC et les FC des stations du réseau échangent entre elles des flux d'information:

- des messages opérationnels pour la manoeuvre du réseau, les liaisons a réaliser, les déplacements de stations, les ordres logistiques et les comptes-rendus d'exécution;
- et des messages techniques pour le transfert des données de configuration du réseau, et la connaissance en temps réel de l'état des liaisons et des équipements.

Conclusion

En conclusion, le réseau tactique de nouveau génération comprend un certain nombre de fonctions:

- Des Services Internet Tactique offerts aux usagers;
- Une fonction Switching et Routing;
- Des équipements Faisceaux Hertziens;
- Des équipements de chiffrement des liaisons COMSEC et de sécurité IPSEC;
- Des Radios de Combat qui peuvent s'intégrer comme usagers mobiles;
- Des outils d'administration et de gestion du réseau.

Horváth Zoltán
horvath.zoltan@zmne.hu

A KIS- ÉS KÖZEPES MAGASSÁGON FELADATOT VÉGREHAJTÓ PILÓTA NÉLKÜLI REPÜLŐGÉP REPÜLÉSI ÚTVONAL TERVEZÉSE DIGITÁLIS DOMBORZAT MODELL (DDM) ALKALMAZÁSÁVAL

Absztrakt

A szerző munkájában bemutatja a pilóta nélküli repülő eszközök (Unmanned Aerial Vehicle, UAV) repülési útvonal tervezésének egy új módszerét. A felszín magassági adatainak ember általi figyelembe vétele a tervezése során körülményes. A cikk ennek az automatizálási lehetőségére világít rá.

The author presents the work of unmanned air vehicles (Unmanned Aerial Vehicle, UAV) flight path planning of a new method. The surface elevation data by taking into account the people in planning difficult. The article highlights the potential for this automation.

Kulcsszavak: *repülésbiztonság, UAV ~ flying safety, UAV*

BEVEZETÉS

A jelenlegi korszerű kis- és közepes magasságon feladatot végrehajtó pilóta nélküli repülőgép már rendelkezik azzal a képességgel, hogy fedélzeti számítógépbe töltött térbeli koordináták alapján önállóan repüli be a részére előzetesen meghatározott útvonalat. Fedélzetére telepített GPS vevő a frissítési rátának megfelelően időről-időre közli a pillanatnyi koordinátákat. A GPS vevő mellett más típusú, pl. barometrikus magasságmérő is szolgáltathat magassági adatot. A GPS adatok, vagy a fedélzetre telepített pitot-cső nyomásmérési adatai alapján kontrollálható a repülési sebesség.

Fent említett fedélzeti mérési adatok viszont nem engednek következtetni a valóságos domborzat (felszín) okozta veszélyre. Útvonaltervezés során a repülési feladatot tervező személy kétdimenziós térkép alapján (papírsíkon, vagy képernyőn) hajtja végre a repülési útvonal tervezését.

Repülés szempontjából alapvető fontosságú a biztonságos, felszín feletti minimális repülési magasság meghatározása. A térképeken az ehhez szükséges információk természetesen rendelkezésre állnak (pl.: szintvonalak formájában), de kiértékelésük időigényes, nehézkes, nagy hibalehetőséggel terhelt.

A térinformatikai adatbázisok – ezen belül a folytonos raszteres Digitális Domborzat Modell (DDM) – alkalmazásával szeretném bemutatni a biztonságosan repülhető útvonalak tervezésének egy lehetőségét.

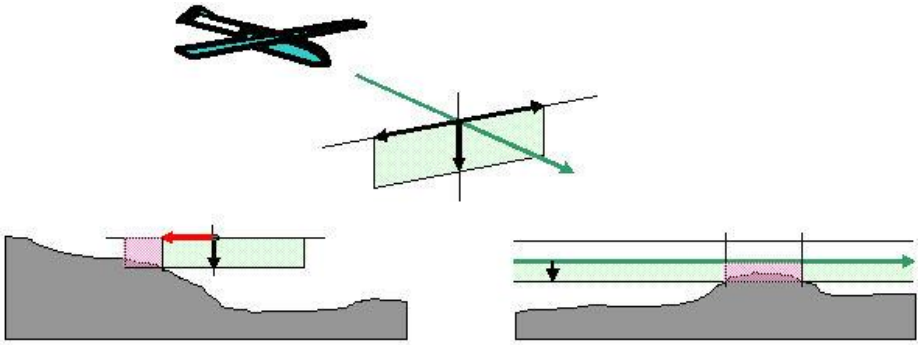
1. HORIZONTÁLIS- ÉS VERTIKÁLIS BIZTONSÁGI TÁVOLSÁGTARTALÉK

Az UAV részére az aktuális megkívánt repülési magasságra vonatkozó adatok csak egy alapfelület feletti magasságként jelentkeznek. Az UAV a turbulencia, széllökések, technikai korlátok miatt elsodródhat a kijelölt útvonaltól, váratlan süllyedés veszélyeztetheti. A

fedélzeti automatika reagálási sebessége és az UAV technikai korlátai meghatározzák a repülési pálya követésének pontosságát.

A feladat-végrehajtás során az UAV környezetében feltételezve egy adott szélességű horizontális- és vertikális távolságtartalékot, melyen belül nem lehet akadály, valamint figyelembe véve az előre látható akadály(ok) átrepüléséhez szükséges emelkedési illetve süllyedési képességet biztonságosan repülhető útvonal tervezhető.

Nem elég körültekintő megoldás az, ha a terep lehetséges legmagasabb pontja fölé emeljük az UAV-t és így kívánjuk a biztonságos magasságtartalékot garantálni, mivel a mélyebben fekvő területek felett felesleges, és pl. a felderítési küldetést meghiúsító magasságon haladhatunk.



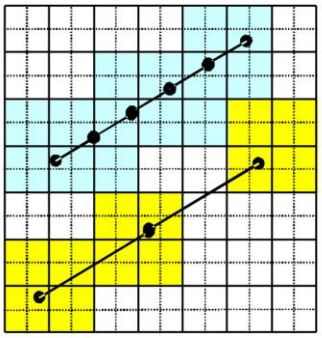
1. ábra: A repülés irányára merőleges horizontális és vertikális biztonsági távolságtartalék

2. HORIZONTÁLIS TÁVOLSÁGTARTALÉK TERVEZÉSE DDM ALKALMAZÁSÁVAL

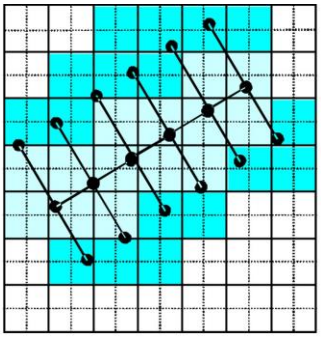
A repülési útvonal vízszintes síkját vizsgálva megállapítható, hogy önmagában nem elegendő a vertikális síkmetszet vizsgálata. A repülőgép a repülést zavaró hatások miatt bizonyosan el fog térni ettől az elméleti vonaltól. A horizontális távolságtartalék biztosítása érdekében tehát nem egy egyenes mentén, hanem egy sávban kell a magassági adatokat értékelni (2. ábra). A metszet mentén virtuálisan úgy kell „megemelni” a magasságot, hogy a megemelt pontból vizsgálva a horizontális távolsági tartalék sávjában a „megemelt” magasság fölé ne emelkedjen akadály (pl.: völgy átrepülése közben az oldalsó hegyoldalak).

Ennek lehetséges módja, hogy az osztópontokon rendre végighaladva a horizontális távolságtartalék határáig, a haladási irányra merőlegesen, a DDM-ből beolvasott magassági értékek közül a maximális magasság kerül figyelembe vételre.

Az útvonal vertikális vetületének irányvektora és normál vektorai az adott útvonalon belül két szomszédos osztópont koordinátái alapján meghatározható (irányváltozás csak a fordulópontoknál következik be).



Megfelelő sűrűségű mintavételezés és alul-mintavételezés



Sáv letapogatása a repülési útvonal mentén

2. ábra: Az értékelés szempontjából feldolgozandó magassági adatok

3. VERTIKÁLIS TÁVOLSÁGTARTALÉK TERVEZÉSE DDM ALKALMAZÁSÁVAL

A vertikális távolságtartalék biztosítása érdekében az előzőekben „megemelt” pontok halmazának magassága tovább növelhető a vertikális távolságtartalékkal.

A vertikális távolságtartalék az UAV-k részére már biztosít egy olyan szabad teret, mely elméletileg repülhető, viszont a merevszárnyú UAV-k emelkedési és süllyedési képessége korlátozott.

4. AZ UAV SÜLLYEDÉSI ÉS EMELKEDÉSI KÉPESSÉGÉNEK FIGYELEMBE VÉTELE

Az UAV süllyedési és emelkedési korlátait figyelembe véve a vertikális távolságtartalék önmagában még nem elég. Az UAV előtt található akadály biztonságos magasságban történő átrepüléséhez időben meg kell kezdeni az utazómagasságról történő emelkedést, illetve az utazómagasságra történő süllyedést.

A vertikális manőverek végrehajtása során a repülési sebesség kézben-tarthatósága korlátoz. Túl meredek süllyedésre kényszerítve az UAV átlépheti a kritikus maximális sebességet, amely szerkezeti károsodáshoz vezethet, vagy tehetetlenségéből adódóan oly mértékben alásüllyedhet az utazómagasságnak, hogy pályája metszi a felszínt. Túl meredek emelkedésre kényszerítve az UAV sebességvesztése következtében áteshet.

5. MINIMÁLIS MEGKÖVETELT REPÜLÉSI MAGASSÁG FIGYELEMBE VÉTELE

Az UAV fedélzetén a repülési feladat végrehajtásához tárolt energia korlátozott. A küldetés végrehajtása során az energiafelhasználás szempontjából leggazdaságosabb üzemmód az állandó magasságon végrehajtott útvonalrepülés (süllyedés során nincs lehetőség energia visszatáplálására, az emelkedés során, a fedélzeten tárolt energia nagy része a helyzeti energia növelésére fordítódik). Küldetés során ezért célszerű a feladat végrehajtás körzetébe történő kijutáshoz, illetve az onnan való visszatéréshez állandó magasságú útvonalrepülés tervezése.

6. A REPÜLÉSI ÚTVONAL ADATAINAK POSZTPROCESSZÁLÁSA

Az UAV részére az eddig tárgyaltak alapján rendelkezésre áll egy biztonságosan repülhető útvonal, amely viszont a felbontás finomsága miatt feleslegesen sok információt tartalmazhat. Ha az információtartalom megőrzése mellett lehetőség van arra, hogy az egymást követő elemi vektorok összevonhatók egyetlen vektorrá, jelentősen csökkenthető a repülési útvonal generálása során létrejövő adatfájl mérete.

A kiindulás alapgondolata az volt, hogy az elemi vektorok által leírt pályaszakasz meddig tekinthető egyenesnek, amely egyetlen vektorral helyettesíthető.

A megvalósításhoz bevezetésre került egy új fogalom. Egyetlen vektorral helyettesíthető azon pályaszakaszt leíró elemi vektorok halmaza, mely vektor által leírt pályaszakasz, és az azt felölelő valamennyi elemi vektorok által leírt pályaszakasz közötti eltérés osztópontonként vizsgálva egy előre meghatározott tűréshatáron belül van.

Számítsuk ki a vizsgált szakasz kiinduló pontja és a vizsgált pont közé kifeszített (v_2), valamint a vizsgált szakasz kiinduló pontja és a vizsgált pontot követő pont közé kifeszített (v_1, feltételezhető egyenes repülési útvonalszakasz) vektorok abszolút értékét és skalárszorzatát. Ezt a műveletet a feltételezhető egyenes repülési útvonalszakasz mentén végezzük el valamennyi osztópontra a kiinduló osztóponttól a vizsgált osztópontig. Ebből meghatározható, hogy van-e olyan osztópont a vizsgált tartományon belül, melynek távolsága a feltételezhető egyenes repülési útvonalszakasztól tűréshatáron kívül van-e (r_{max}) {1}.

$$r_{\max} \geq \sqrt{\left|\bar{v}_2\right|^2 - \left(\frac{\bar{v}_1 \cdot \bar{v}_2}{\left|\bar{v}_1\right|}\right)^2} \qquad \{1\}$$

Ha valamennyi osztópont távolsága a feltételezhető egyenes repülési útvonalszakasztól tűréshatáron belül van, akkor az még összevonható egy egyenessé (elemi vektorai helyett egyetlen vektorral helyettesíthető), beolvasva a következő vizsgált pontot és az azt követő pontot, újra elvégezhetjük a vizsgálatot. Ha valamely osztópont távolsága a feltételezhető egyenes repülési útvonalszakasztól tűréshatáron kívül van, akkor a repülési útvonal már nem egyenes. Az eddig számított feltételezhető egyenes repülési útvonalszakasz koordinátáit elmentve (kiinduló pont, vizsgált pont viszonylatában), az új feltételezhető egyenes repülési útvonalszakasz kiinduló pontja legyen a vizsgált pont.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Ezek alapján a repülési útvonal tervezésének egy lehetséges módja a következő:

- megfelelő finomságú mintavétel alapján a repülési útvonal osztópontokkal történő felosztása;
- a minimális repülési magasság meghatározása a horizontális távolságtartalék biztosítása érdekében;
- a repülési magasság szükség szerinti növelése a vertikális távolságtartalék biztosítása érdekében;
- a repülési magasság szükség szerinti növelése az UAV süllyedési és emelkedési képességeit figyelembe véve;

- a repülési magasság szükség szerinti növelése, ha előírt magasságú útvonalrepülés a feladat.

Megvizsgáltam a biztonságosan berepülhető útvonal tervezésének automatizálási lehetőségét. A tervező kétdimenziós síkon látja a háromdimenziós teret. Ebből adódóan a horizontális távolsági tartalék és a vertikális távolsági tartalék figyelembe vétele aprólékos (időigényes) munkát, vagy nagy tapasztalatot igényel. Az ember, mint szubjektum önhibáján kívül nem vesz figyelembe olyan, a tervezés szempontjából fontos adatokat, melyek veszélyeztetik a repülés biztonságát.

Az UAV küldetésének előkészítése során a küldetés útvonalát tervező személy a rendelkezésére álló, számára nehezen feldolgozható adatok alapján dönt. Belátható, hogy a rendelkezésre álló adatok gyors és az elvárt mértékig helyes feldolgozása, majd a fedélzeti elektronika által megkívánt formára hozása a tervező számára emberi erővel gyakorlatilag lehetetlen. Az útvonaltervezést a fent leírt elgondolások alapján át lehet alakítani.

FELHASZNÁLT IRODALOM:

[1] Dr. Detrekői Ákos – Dr. Szabó György, Bevezetés a térinformatikába, Nemzet Tankönyvkiadó, Budapest, 1995

[2] Zentai László, Számítógépes térképészet, ELTE Eötvös kiadó, Budapest, 2000

[3] Micropilot UAV autopilots homepage, http://www.micropilot.com/

[4] UAV Flight Systems homepage, http://www.uavflight.com/

Horváth Zoltán
horvath.zoltan@zmne.hu

AZ UAV REPÜLÉS STABILIZÁLÁSÁNAK KÉRDÉSEI

Absztrakt

A szerző bemutatja a pilóta nélküli repülő eszközök (Unmanned Aerial Vehicle, UAV) repülés stabilizálásának egy új módszerét. Rámutat, hogy egy szenzor alkalmazásával hogyan lehet növelni a repülés stabilitását, és ez milyen hatással van ez az irányítást végzőre. Példaként bemutat egy általa tervezett szenzort.

The author describes the unmanned air vehicles (Unmanned Aerial Vehicle, UAV) flight to a new stabilization method. Indicates that a sensor that how to increase the stability of flight, and what effect does this have to control investigator. As it shows an example of planned sensors.

Kulcsszavak: *UAV, repülésbiztonság ~ UAV, air traffic safety*

BEVEZETÉS

A jelenlegi korszerű kis- és közepes magasságon feladatot végrehajtó pilóta nélküli repülőgépek repülése során a repülés horizontális irányának változtatása, a külső hatásokra való gyors reagálás tapasztalt szakembert igényel. Fordulóba vitt repülő eszköznél, illetve, pl. széllökés által kibillentett repülő eszköz esetén az eszközre ható erők figyelembe vétele létfontosságú.

A merevszárnyú repülőeszközök háromdimenziós pozíció váltását a tér három irányának megfelelő (a függőleges- és vízszintes vezérsíkon, valamint a szárnyakon található) kormánylapokkal hajtják végre.

A repülés során a fordulók kivitelezése, a váratlan (széllökés által keltett) pozícióváltás hatására megváltozik a szerkezetre ható erők iránya. Ennek következménye, hogy nem irányváltoztatás, hanem manőver kivitelezése a megoldás (több irányú manőver egyidejű, mérlegelt kivitelezése).

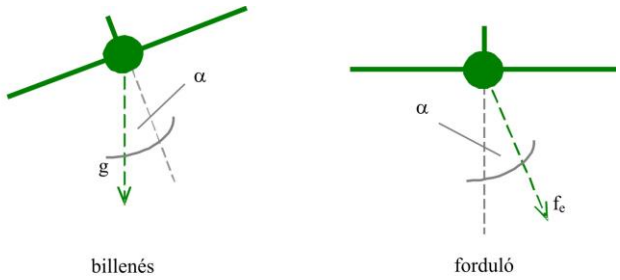
Ez a cikk olyan szenzor megalkotásáról, alkalmazható szenzorok kutatásáról szól, melyek által biztosítható, hogy a repülő szerkezet automatizált módon, a rá ható erők függvényében automatikusan vegye fel azt a pozíciót, mely által irányítása csak irányváltást és nem manőver kivitelezését igényelje. Ez által a kezelőszemélyzettel szemben támasztott követelmények csökkenthetők, a repülés biztonsága és a repülő eszköz autonómiája növelhető.

1. A REPÜLŐ SZERKEZETRE HATÓ ERŐ ÉRZÉKELÉSE

Forduló, vagy széllökés hatására fellépő megbillenés kompenzálásának automatizált kivitelezése egyszerűsíti a pilóta feladatát. A repülő szerkezet szárnysíkja, ha merőleges a repülő eszközre ható erő irányával, akkor elegendő a függőleges vezérsíkra kiadott „jobbra - balra” parancs a forduló kivitelezéséhez. A szükséges bedöntésről a repülő eszköz

gondoskodik. Kivitelezésének alapja, hogy a repülőeszköz szárnyai által kijelölt függőleges sík és a repülőszerkezetre ható erők irányának összehasonlításaként hibajel keletkezzen.

Billenés esetén a szárnysíkot kell összehasonlítani a nehézségi gyorsulásvektor irányával, vissza kell térni vízszintes síkú repülésre. Forduló esetén viszont a repülő szerkezetre ható eredő erő kiegészül a centripetális erővel, melyet érzékelni kell (1. ábra).



1. ábra: A repülőszerkezet és a rá ható erők viszonya

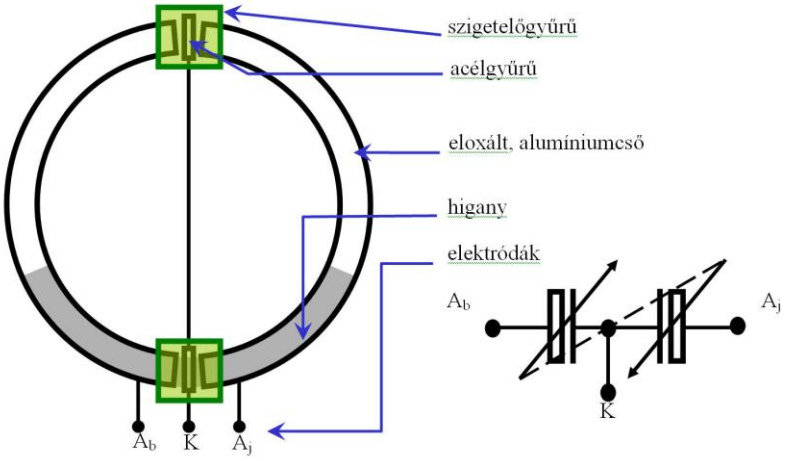
Az érzékelő eszköz repülő szerkezetbe történő fix beépítést követően a billenés detektálható. Forduló végrehajtása során a következő egyszerű számítás mutat rá a detektálás szükségességére.

Például, ha:
- a repülés sebessége = 100 km/h;
- a fordulás sugara = 100 m;

akkor:
- a centripetális gyorsulás = 7,72 m/s^2;
- a repülő szerkezetre ható nehézségi és centripetális gyorsulás összege = 12,48 m/s^2
- az erő iránya a függőlegeshez képest = 38,19°.

2. AZ ÉRZÉKELŐ ALKATRÉSZ FELÉPÍTÉSE

A rendszer fő elemeként egy olyan változó paraméterrel rendelkező alkatrész kialakítása a cél, mely megfelelő finomsággal képes közölni a repülő szerkezet bedőlésének mértékét, és nincs halmozódó hibája. Kapacitás változás előállítására egy ívben (pl. kör alakú vezetőcsőben) meghajlított csőben folyó anyag erre képes (2. ábra). A továbbiakban az alkatrész kialakítását indokolom.



2. ábra: Az érzékelő alkatrész felépítése és helyettesítő képe

2.1. Szerkezeti kialakítás

A 2. ábrán látható, hogy az érzékelő két, egymástól elszigetelt félköríven hajlított eloxált alumíniumcsőre épül (anódok). Az acélgyűrűk (katód) csak a higannyal létesítenek elektromos kontaktust. A szigetelőgyűrűk a rendszer zártságát biztosítja.

Ez alapján kapunk egy olyan kondenzátorpárt, mely kondenzátorok kapacitásváltozása, síkjában történő elfordulás hatására ellentétes irányú. A kondenzátorok kapacitása és kapacitás változása a síkkondenzátorok mintájára könnyen számítható. Az ellentétes irányú változás kínálja a wheastone-hídban történő alkalmazást.

2.2. A kondenzátorok kialakítása

Anódként az alumíniumcső alkalmazása kis fajsúlya miatt ideális. Eloxációval (kémiai oxidáció, anódos oxidáció) az alumínium felületén szigetelőréteg hozható létre (Al_2O_3), mely szigetelőréteg (dielektrikum) a technológia függvényében 1…50 mikrométer vastagságú, lágy, hajlítható, vagy korund keménységű lehet. Az Al_2O_3 relatív permittivitása 7. A cső belső előmaratásával a fegyverzet felülete akár egy nagyságrenddel növelhető.

Az alumínium erős redukálószer, a higany közepes oxidálószer. Ez biztosítja, hogy az érintkezés során az Al_2O_3 szigetelőréteg stabil, a higany nem oldja fel, viszont az így kialakított eszköz egy elektrolit kondenzátor, tehát polaritásérzékeny. Hibás polarizáció hatására a kialakított Al_2O_3 szigetelőréteg feloldódik, és a higany közvetlen kapcsolatba kerül az alumíniummal.

Katódként folyadékként tökéletesnek tűnik a higany fegyverzetként történő alkalmazása. Feltételezzük, hogy az UAV nem megy át negatív gyorsulásba. Ekkor a higanycsík a csőben mindig „alul”, a gravitáció és a centripetális gyorsulás haladás irányára merőleges vektorkomponensének hatására veszi fel pozícióját (a cső aljára folyik, de a fordulóban bedől). Alkalmazását jó vezetőképessége is indokolja. Nagy tömege és nagy felületi feszültsége okán a fedélzeti rezonancia nagy valószínűséggel nem tépi szét a folyamatos katódcsíkot. A gyorsulásvektor változására gyorsan reagál. Nem nedvesít. Széles hőmérséklettartományban (-38 °C ÷ 357 °C) folyékony.

Viszont ne felejtkezzünk meg néhány hátrányáról. Ha az Al_2O_3 réteg sérülése folytán közvetlen kapcsolatba kerül az alumíniummal, vele amalgámot képez. A szigetelőrétegnek tökéletesnek kell lennie. Ugyan ez az indoka annak, hogy a higannyal az elektromos kontaktust acélgyűrűn keresztül terveztem, ugyanis a higany az acéllal nem képez amalgámot. Másik hátránya az, hogy erősen mérgező és illékony, ezért mindenféleképpen zárt rendszerben lehet csak alkalmazni.

2.3. Az érzékelő modellezése

A számítások során az alábbi paraméterek figyelembe vételével néhány elméleti számítás eredménye:

Adatok_1:

- a cső görbületi sugara: 2,5 cm;
- a cső belső üregének átmérője: 5 milliméter;
- a higanycsík ebből 80 fokos nyílásszöget tölt fel (ekkor a higany tömege: 9.28 gramm);
- szigetelőréteg (Al_2O_3) vastagsága: 20 mikrométer;
- katódbevezetés szigetelőgyűrűjének szélessége: 3 milliméter.

dőlés:	10 fok balra	5 fok balra	1 fok balra	0 fok vízszint	1 fok jobbra	5 fok jobbra	10 fok jobbra
C_{bal}	0.989 nF	0.883 nF	0.798 nF	0.776 nF	0.755 nF	0.670 nF	0.564 nF
C_{jobb}	0.564 nF	0.670 nF	0.755 nF	0.776 nF	0.798 nF	0.883 nF	0.989 nF

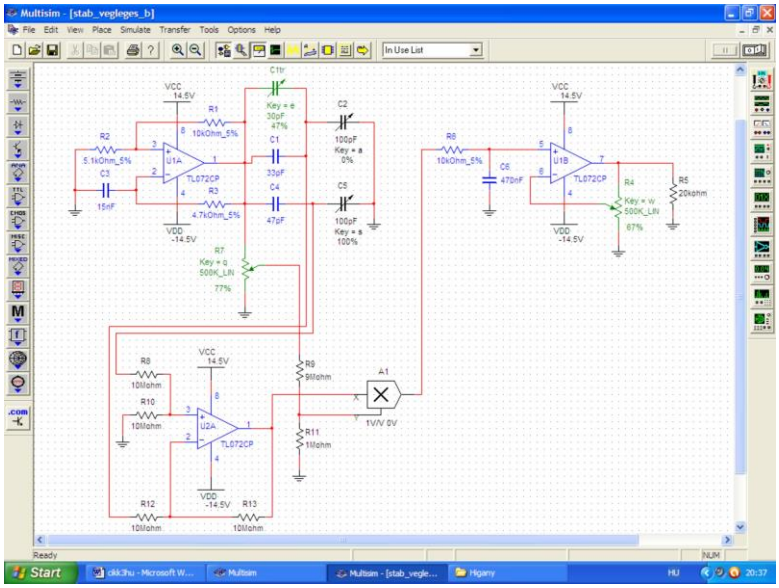
Adatok_2:

- a cső görbületi sugara: 5 cm;
- a cső belső üregének átmérője: 4 milliméter;
- a higanycsík ebből 60 fokos nyílásszöget tölt fel (ekkor a higany tömege: 8.91 gramm);
- szigetelőréteg (Al_2O_3) vastagsága: 10 mikrométer;
- katódbevezetés szigetelőgyűrűjének szélessége: 5 milliméter.

dőlés:	10 fok balra	5 fok balra	1 fok balra	0 fok vízszint	1 fok jobbra	5 fok jobbra	10 fok jobbra
C_{bal}	2.524 nF	2.184 nF	1.912 nF	1.844 nF	1.776 nF	1.504 nF	1.165 nF
C_{jobb}	1.165 nF	1.504 nF	1.776 nF	1.844 nF	1.912 nF	2.184 nF	2.524 nF

3. EGY VEZÉRLŐ ÁRAMKÖR LEHETSÉGES KIALAKÍTÁSA

A továbbiakban egy áramkör felépítését és működését mutatnám be, mely alkalmas lehet irányítási funkciók ellátására (3. ábra).



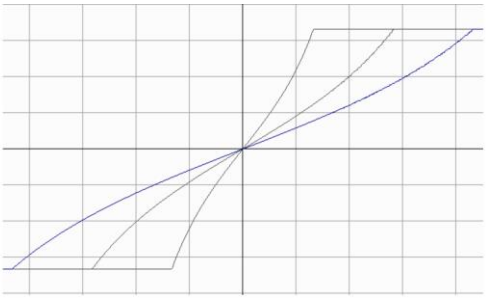
3. ábra: Az érzékelő eszközt alkalmazó szenzor áramköri rajza

Az általam alkalmazott áramkör ±15V tápfeszültséget igényel ennek kialakítása példaként LM2700 step-up PWM DC/DC konverterrel megvalósítható, katalógusában a szükséges kapcsolási rajz és a kimenőfeszültség beállításához szükséges feszültségosztó számítása megtalálható.

A szenzor működése a következő:

- U1A műveleti erősítőre felépített astabil multivibrátor 100kHz-es, ±12V-os négyszögjelet állít elő egyrészt az érzékelő elemet tartalmazó wheadstone-híd gerjesztéséhez, másrészt csatlakozik egy szorzóáramkör egyik bemenetéhez. A szorzóáramkör bemeneti amplitúdója R7 potenciométerrel szabályozható. Erre a szorzóáramkör linearitásának biztosítása érdekében van szükség.
- C1, C2, C4, C5 wheadstone-híd kiegyenlítését biztosítja C1tr trimmerkondenzátor. Erre még a küldetés kezdete előtt a földön, a hibajel nullázása érdekében van szükség (vízszintes szárnysík esetén).
- U2A műveleti erősítő és A1 szorzóáramkör egy AD633 négynegyedes szorzóáramkört szimulál. Egyik bemenete U1A multivibrátor leosztott jele, másik a wheadstone-híd két hídpontja. Az alapjelhez képest a hídpontról levett feszültség fázisa (jobbra, vagy balra mutat a gyorsulásvektor a szárnysíkhoz képest) 0° vagy 180° fázisugrást mutat, amplitúdója közel lineárisan arányos a hibával.
- Az alapjel fel és lefutási hibáiból eredő feszültségingadozást R6, C6 integrátor simítja ki.

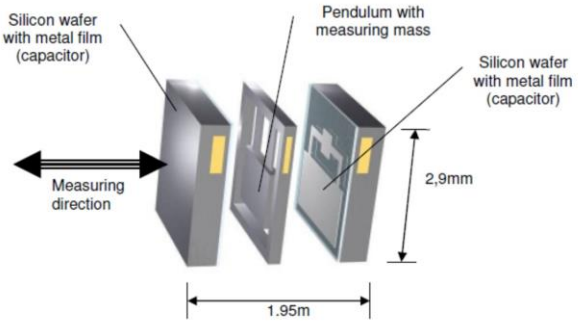
- U1B-re épített erősítő erősítése R4 potenciométerrel szabályozható. Meghatározza, hogy a maximális ±12V kimenő feszültség mekkora szögtartományban oszoljon meg.
- Az áramkör transzferkarakterisztikája (függőleges: hibafeszültség ±12 V, vízszintes: erőhatás iránya ±90°) a 4. ábrán látható.



4. ábra: Az áramkör transzfer karakterisztikája

4. EGYÉB LEHETŐSÉGEK

Az elektronikai piacon fenti problémák megoldására számos alkatrész fellelhető, melyek különböző specifikációknak megfelelően képesek elfordulás, vagy gyorsulás mérésére. Példaként a KELAG Künzli Elektronik AG számos változatát gyártja az erre a célra is alkalmazható szenzoroknak. Ezen szenzorok működési elve is a kapacitásváltozás mérésén alapul (5. ábra).



5. ábra: A szenzor „lelke”

Ezen érzékelők a kapacitásváltozás következtében keletkező hibajelet típustól függően analóg és digitális formában (soros és párhuzamos formában) is képesek közölni.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK:

A bemutatott jeladók könnyen integrálhatók a fedélzeti rendszerbe. Könnyűek, olcsók egyszerű felépítésűek.

Alkalmazásuk során automatikusan gondoskodnak arról, hogy a repülő szerkezetre ható erő legyen merőleges a szárnysíkra, ezáltal növeli a repülés stabilitását, egyszerűsíti a repülés irányítását, szűkíti a forduló sugarát.

A modellezéshez, tervezéshez és teszteléshez alkalmazott szoftverek:

- Multisim 2001 Education, áramkör tervező- és analizáló program;
- Borland Pascal 7.0 szoftverfejlesztő környezet.

FELHASZNÁLT IRODALOM:

[1] Az alumínium felületkezelése, http://www.sasovits.hu/cnc/ontes/Al_feluletkezeles.pdf

[2] Az aluminium eloxálása, http://elektron.uw.hu/elektro/egyeb/eloxalas.pdf

[3] Eloxálás Rádióamatőrök zsebkönyve, Műszaki Kiadó 1967 http://www.sasovits.hu/cnc/irodalom/eloxalas.pdf

[4] Sulinet: Passzivitás és korrózió, http://www.sulinet.hu/tart/fncikk/Kidb/0/30271/index.html

[5] AD 633: Low Cost Analog Multiplier, http://www.analog.com/static/imported-files/data_sheets/AD633.pdf

[6] LM2700 600kHz/1.25MHz, 2.5A, Step-up PWM DC/DC Converter, http://www.national.com/ds/LM/LM2700.pdf

[7] Borbély Gábor: Elektronika II. (A műveleti erősítő és kapcsolástechnikája) http://www.szechenyi-zala.sulinet.hu/dokumentumok/Tananyag/elektronika/Elektronika2.pdf

[8] Precision ±1.7g Single-/Dual-Axis iMEMS® Accelerometer, AXDL204 http://www.analog.com/static/imported-files/data_sheets/ADXL204.pdf

[9] Application manual: Acceleration, inclination an vibration sensor SCA series http://www.kelag.ch/industriesensoren/besch/SCA_UG_E.pdf

[10] Preliminary SCA1000 and SCA1020 Series http://www.vti.fi/midcom-serveattachmentguid-e1431941e79a12e44ed615e204785f58/SCA1000_accelerometer_180105.pdf

[11] The SCA103T Differential Inclinometer Series http://www.vti.fi/midcom-serveattachmentguid-c914062fbf2c76a3d7cff8016e0dc09a/SCA103T_inclinometer_datasheet+_8261700A.pdf

[12] SCA610 Series, Accelerometer/Inclinometer, http://www.vti.fi/midcom-serveattachmentguid-3e9dbe96363583705f8e7d7923d5f9bc/SCA610_accelerometer_Rev_3.pdf

[13] The SCA61T Inclinometer Series, http://www.vti.fi/midcom-serveattachmentguid-2b9fadebe6fa4a0c24f144cd55fda22d/SCA61T_inclinometer_datasheet_8261900A.pdf

[14] SCA620 Series, Accelerometer, http://www.vti.fi/midcom-serveattachmentguid-97369a0919e2987f574d12a7f1f41e45/DN_accelerometer_sca620_260804.pdf

[15] The SCA100T Dual Axis Inclinometer Series, http://www.vti.fi/midcom-serveattachmentguid-30e230919288bbb060588d83d7501b7f/SCA100T_inclinometer_datasheet_8261800A.pdf

Horváth Zoltán
horvath.zoltan@zmne.hu

DIGITÁLIS DOMBORZAT MODELL ALKALMAZÁSA A KIS- ÉS KÖZEPES MÉRETŰ PILÓTA NÉLKÜLI REPÜLŐGÉPEK BIZTONSÁGÁNAK NÖVELÉSE, KÉPESSÉGEINEK FEJLESZTÉSE TERÉN

Absztrakt

Jelen közlemény a Katonai Műszaki Doktori Iskolában elvégzett kutatásokat mutatja be.

The article provides an overview of my research activity about the programme application of a Digital Terrain Model; Increased safety of small and middle-size unmanned aerial vehicles; Development of its capabilities.

Kulcsszavak: *Digitális Domborzat modell, UAV ~ Digital Terrain Model, UAV*

1. BEVEZETÉS, TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A pilóta nélküli légi járművek (továbbiakban: UAV) alkalmazása napjainkban egyre nagyobb teret hódít. Gyors fejlődésük és egyre elterjedtebb alkalmazásuk számos, a hagyományos repülő eszközök üzemeltetésével szembeni előnyének köszönhető. Felderítő és kutatótevékenységet folytathatnak nehezen megközelíthető, vagy veszélyes helyszíneken. Biztonságos távolságról irányítható a küldetés végrehajtása, az alkalmazók életének, testi épségének veszélyeztetése nélkül. Üzemeltetése és üzemben tartása költséghatékonyabb, küldetéshez való előkészítésének és az utólagos karbantartás elvégzésének időtartama rövidebb, mint az ember vezette repülő eszközöké. Az alkalmazói képzés olcsóbb – lényegesen kevesebb időt és üzemórát vesz igénybe – mint a pilóták felkészítése. Az alkalmazói alkalmasság nincs a légi üzemeltetéshez szükséges egészségügyi követelményhez kötve. A légi személyzet és a hozzájuk kapcsolódó számos eszköz, mivel nem a fedélzeten foglal helyet, a méretezés és kialakítás új perspektíváit nyitotta meg, javítva a hasznos teher – teljes tömeg arányon.

Sok előnye mellett elterjedésének és alkalmazásának hátrányairól sem szabad megfelejtkezni. Alkalmazhatóságukat, elsősorban a biztonságos repülés végrehajtását, hatótávolságukat, befolyásolhatja a földi irányítás és a fedélzet közötti kommunikáció2 stabilitása.

Újabb biztonsági problémaként merül fel az, hogy a magára hagyott, vagy magára maradt UAV-nak milyen lehetőségei vannak arra, hogy újra fel tudja építeni a kommunikációt, vagy önállóan, biztonságosan végre tudja hajtani feladatát. Vannak olyan feladatok (pl. ortofotók készítése), melyek végrehajtására az UAV-k legnagyobb része jelenleg még alkalmatlan.

Ennek okaiként említem – kis tömegéből és méretéből adódóan – a fedélzeti hasznos terhelhetőségének korlátozottságát, a repülés stabilizáltsági szintjét és a viszonylag kis repülési magasságot.

Kutatásaim során a kis- és közepes magasságon4 feladatot végrehajtó pilóta nélküli repülőgépek repülésbiztonságának és képességfejlesztésének kérdéseit tárgyalom. Van-e lehetőség a repülésbiztonság növelésére (kommunikációs instabilitás és nem megfelelően átgondolt útvonalterv végett bekövetkező események elkerülésére)? Fontos kérdés, hogy

mindez kivitelezhető-e anélkül, hogy tovább nőne a hasznos terhek tömege? Megoldható-e, hogy a kis- és közepes magasságon feladatot végrehajtó UAV által, tetszőleges helyzetben készített perspektivikus digitális légi fényképeket utólagos feldolgozással átalakítsuk ortofoto képpé?

A repülés biztonságáról lemondani nem szabad. Egy küldetés során az UAV-nak minden körülmények között végre kell hajtania a feladatát, és ha eleve nem egyszeri alkalmazásra tervezték, akkor vissza kell térnie. Ha ez az elv csorbát szenved, ez – minden előnye ellenére – akadályozhatja alkalmazásának elterjedését. Esemény során kárt okozhat, elvész az eszköz és az általa gyűjtött adat, illetéktelen kezekbe kerülhet, balesetet okozhat.

Növelné az UAV értékét, ha a már meglévő struktúrára építve, az egyébként csak speciális és költséges rendszerek által végzett feladatok ellátására is képes lenne. Megoldás lehet – a beépített eszközök tömegének korlátozottsága miatt – a „tömeg nélküli eszközrendszer", vagyis a számítógépes programok és adatbázisok alkalmazása.

Kutatásaimtól olyan eredményeket vártam, amelyek összességében biztonságosabbá teszik az UAV-k feladat végrehajtását, és kibővítik képességeiket, lehetőségeiket. Műszaki kutatásaim – a küldetések tökéletesebb végrehajtása érdekében – három fő kérdésre irányulnak:

- hullámterjedési modellek elemzésével a földi irányítópont ellátottsági körzetének meghatározására;
- előzetesen tervezett fordulópontok6 alapján a biztonságosan repülhető magasságú útvonal meghatározására, és ez alapján a terepkövető repülési mód kidolgozására;
- a perspektivikus digitális légi fényképek perspektivikus és domborzat által okozott torzításainak kompenzálásán keresztül digitális ortofotók előállítására, azok ortofoto térképekké történő szintetizálására irányulnak.

Kutatásaim során a Digitális Terepmodell (továbbiakban: DTM) és a Digitális Domborzat Modell (továbbiakban: DDM) által nyújtott lehetőségek kiaknázásán keresztül hoztam létre ezen funkciókat és feladatokat, amelyek a földi irányítópont és/vagy az UAV fedélzeti számítástechnikai apparátus feladatrendszerébe beintegrálhatók.

Munkám – kiegészítve a már elért eredményeket – meglévő struktúrára építve egészítheti ki az UAV repülésbiztonságának, képességei fejlesztésének lehetőségeit.

2. KUTATÁSI CÉLOK

1. Annak vizsgálata, hogy a földi irányító pont és az UAV viszonylatában a kommunikáció stabilitása – különböző irányítási modellek esetén – miként hat a küldetés sikeres végrehajtására, a repülés biztonságára. Elemezni az egyes hullámterjedési modellek alkalmazhatóságát, és javaslatot tenni, hogy a DDM alkalmazásával előállított ellátottsági- és árnyékdiagramok – növelve a küldetés végrehajtásának sikerességét, a repülés biztonságát – miként vonhatók be az UAV küldetésének tervezési, végrehajtási folyamatába.

2. Rávilágítani, hogy a repülések tervezése és végrehajtása során a háromdimenziós tér kétdimenziós megjelenítéséből (térkép, monitor) adódóan a repülési útvonalak jelenleg folyó tervezése nem elég körültekintő megoldás. Javaslatot tenni, miként lehet síkkoordináták alapján meghatározott repülési útvonalakból térbeli koordináták által leírt, – a repülés biztonságát fenyegető domborzat hatását elkerülő – biztonságos magasságú repülési útvonalakat tervezni, hogyan lehet megvalósítani az automatikus terepkövető módú repülést.

3. Bizonyítani, hogy a DDM és alkalmazására kifejlesztett program(ok) képesek kompenzálni a terepdomborzat torzító hatását, a digitális légi fényképek perspektivikus torzítását, általuk egymáshoz illeszthető ortofotók állíthatók elő viszonylag egyszerű, kis költségigényű módszerrel.

3. ALKALMAZOTT KUTATÁSI MÓDSZEREK

Irodalomkutatásra épülő információk és adatok összegyűjtése és rendszerezése mellett felhasználtam a megfigyelést és a kritikai adaptációt, majd a kutatások másodelemzésével, az összefüggéseknek az analízis és szintézis, az indukció és dedukció, a modellezés és szimuláció módszereinek alkalmazásával törekedtem kutatási céljaim elérésére és megvalósítására.

Fő feladatként az irodalomkutatásra építve algoritmusokat, eljárásokat dolgoztam ki.

Az általam megalkotott algoritmusok és eljárások tesztelésére, működésük megfigyelésére, a keletkező adatok analizálására Borland Pascal 7.0 fejlesztői környezetben számítógépen futtatható programokat hoztam létre. A programok futtatási eredményei lehetőséget biztosítottak a bemeneti paraméterváltozás hatásának elemzésére, következtetések levonására.

A DTM és a DDM kezelését két modell alkalmazásán mutatom be, melyek felbontásuk és koordináta rendszerük alapján is különböznek. A rádiócsatorna bemutatását DTM-200 adatbázison (Gauss-Krűger vetületi rendszer), az útvonaltervezést DDM-50 adatbázison (EOV10 vetületi rendszer) végeztem.

A perspektivikus digitális fényképek feldolgozását (koordináta meghatározása) generált DDM adatbázison végeztem.

Az irodalomkutatáson túl, részt vettem olyan tudományos konferenciákon, szimpóziumokon, ahol a téma, illetve az ezt övező kapcsolódó határterületek kerültek megvitatásra.

Mindezeken kívül konzultációkat folytattam az adott szakterület prominens szakértőivel, tervezőivel, felhasználóival, akik információikkal, tanácsaikkal, kérdéseikkel és további tudományos igényű probléma felvetéseikkel, valamint javaslataikkal nagyban hozzájárultak és segítették munkám elvégzését.

4. KÖVETKEZTETÉSEK

Az UAV-k fejlődését és az ezzel foglalkozó tudományterület létezését napjainkban már senki nem kérdőjelezi meg. Az adott tématerület kutatása multidiszciplináris tudomány, több mérnöki kutatási területet egyesít.

Kutatásaim tárgyát a kis- és közepes magasságon feladatot végrehajtó pilóta nélküli repülőgépek repülésbiztonságának növelése, képességeinek fejlesztése képezte. A repülésbiztonság növelése érdekében megvizsgáltam a rádiócsatorna modellezésének lehetőségeit, kutatva, hogy milyen módon lehet meghatározni azon terepszakaszokat, ahol az összeköttetés bizonytalanná válhat.

Kutattam, hogy milyen módon lehet elkerülni az előzetes útvonaltervezés során bevitt szubjektív emberi hibákat, figyelembe venni a küldetést fenyegető terepdomborzat okozta veszélyeket, és ennek eredményeként megalkottam a terepkövető repülési mód feltételrendszerét.

Nagyon lényeges kérdés ezen eredmények további használhatósága szempontjából, hogy ezek a programok, adatbázisok implementálhatók-e a rendelkezésünkre álló, vagy beszerzésre tervezett pilóta nélküli repülőgép rendszerre. Amennyiben nem, akkor csak egy különálló számítógépen futtathatók az összeköttetést vizsgáló, illetve az útvonaltervező

programok. Ha egy meglévő, vagy fejlesztés alatt álló rendszer szabadon bővíthető, akkor ezen programok korábban nem látott, például vészhelyzet kezelő algoritmusok megvalósításához nyújtanak alapot.

A kis- és közepes magasságon feladatot végrehajtó pilóta nélküli repülőgépek lehetőségei, a fedélzet hasznos terhelhetősége korlátozott. Megvizsgáltam, miként lehet kivitelezni az UAV-k által készített légi fényképek ortofoto fényképekké alakítását. Ez a lehetőség üzemeltetési költség, kezelő személyzet képzettsége, gyors reagálás és végrehajtás szempontjából a hagyományos eljárásokhoz képest gyorsabb, költséghatékonyabb.

A kutatásaim során feltevéseim, megfogalmazott algoritmusaim kivitelezhetőségének ellenőrzésére kísérletként előre berendezett helyszínen fényképeket készítettem, számítógépes programokat írtam és futtattam valóságos, illetve számítógépes program által generált domborzatmodellt alkalmazva.

Kutatásaim során definiáltam a meglévő architektúrára építhető és integrálható eljárások és algoritmusok egész sorát. Olyan eljárásokat, algoritmusokat fogalmaztam meg, melyek a tervezés, szervezés és kivitelezés folyamata során akár a földi irányítópont számítástechnikai apparátusába, akár az UAV fedélzeti számítógépébe beépíthető, növelve a repülés biztonságát, egyszerűsítve a tervezés és végrehajtás feladatait, bővítve az UAV lehetőségeit, mely által más, költségesebb erőforrások igénybevétele mellőzhető.

Összességében tehát három látszólag egymástól meglehetősen távol álló szakmai probléma vizsgálatát végeztem el, amelyek közös alapja a Digitális Domborzat Modell által nyújtott lehetőségek, megközelítési módok alkalmazása volt, közös eredménye pedig a pilótanélküli repülőgépek biztonságosabb bevetéstervezése, technikai lehetőségeinek növelése lett.

Mindhárom kutatási részterület napjainkban teljesen újdonságnak számít, a kis- és közepes magasságtartományban repülő pilóta nélküli eszközök fejlesztése, alkalmazása területén – legjobb tudomásom szerint – ilyen vizsgálatokat, tervezési eljárásokat, képfeldolgozási folyamatokat nem végeznek.

5. A KUTATÁSOK ÚJ TUDOMÁNYOS EREDMÉNYÉNEK TARTOM

1) a kis- és közepes magasságon feladatot végrehajtó pilóta nélküli repülőgépek biztonságos irányításához szükséges rádiócsatorna diffrakciós terjedési modelljeinek vizsgálatával és az ezekhez készített szimulációs program eredményeinek elemzésével annak megállapítását, hogy a Deygout modell alapján készített ellátottsági- és árnyékdiagramok alkalmazása szükségszerű, velük növelhető a repülés biztonsága;

2) a pilóta nélküli repülőgép repülési profiltervező rendszerének elméleti kidolgozását, a gyakorlati modell számítógépes megalkotását, amely a DDM alkalmazásával lehetővé teszi az UAV „terepkövető” repülési módjának megvalósítását, az operátor által bevitt szubjektív, útvonal-tervezési hibák kiküszöbölését;

3) azon elméleti alapok kidolgozását és gyakorlati kísérletekkel való igazolását, amely alapján a kis- és közepes magasságon készített – a domborzat által torzított – perspektivikus fényképek megfelelő követelmények teljesülése esetén ortofoto képpé transzformálhatók, a transzformált képek egymáshoz illesztésével ortofoto térkép hozható létre, mely növeli az UAV alkalmazási lehetőségeit.

6. AJÁNLÁSOK, GYAKORLATI FELHASZNÁLHATÓSÁG

Munkám során rámutattam a kis- és közepes magasságon feladatot végrehajtó pilóta nélküli repülőgépek küldetéstervezésének problematikájára, a képességek fokozásának lehetőségére.

Az összeköttetés folyamatosságát figyelembe véve, a rádiócsatorna átjárhatóságát vizsgálva kiderült, hogy az általam vizsgált terjedési modellek jól algoritmizálhatók, a terjedési modellek és a domborzatmodellek alkalmazásával az összeköttetés megvalósíthatósága vizsgálható, de ez csak egy elméleti sík. Az egyes modellek viselkedése eltérő. Célszerű terepen végzett mérések és az egyes terjedési modellek eredményeinek összevetése, értékelése annak érdekében, hogy a gyakorlati mérésekkel alátámasztható legyen, hogy a Deygout modell a legalkalmasabb ellátottsági- és árnyékdiagram készítéséhez.

Az ellátottsági- és árnyékdiagramok alkalmazása a tervezés és végrehajtás során a küldetés sikeressége, helyes tervezése szempontjából nagy segítséget nyújthat. Célszerűnek tartom az ellátottsági- és árnyékdiagramok repülési útvonal tervezési folyamatába történő bevonását. A domborzat figyelembe vételével kidolgozott repülési útvonal tervezési lehetősége jelentősen csökkentheti a tervező állomány tevékenységének bizonytalanságát. Célszerűnek tartom a domborzat figyelembe vételének alkalmazását az útvonal tervezése során, összehasonlítását a hagyományos tervezési eljárással a hatékonyság és biztonság szemszögéből.

Javaslom a domborzat figyelembe vételével kidolgozott repülési útvonalak berepülés útján történő tesztelését, mely által kimutatható a fedélzeti rendszer működése és a repülési feladat végrehajthatósága közti diszharmónia.

A kis- és közepes magasságú repülés során készített perspektivikus képek modellezése során felmerülő, hibát okozó tényezők csak valóságos körülmények között szűrhetők ki.

Kutatásaim révén megfogalmazott eredményekkel felhívom az UAV kutatók és tervező mérnökök figyelmét a földi irányító pont és a fedélzeti számítógép által alkalmazott szoftverrendszer moduláris kiegészíthetőségének lehetőségére.

Jobbágy Szabolcs
jobbagy.szabolcs@zmne.hu

A MAGYAR HONVÉDSÉG SZEREPVÁLLALÁSA A BIZTONSÁG ÉRTELMEZÉSÉNEK TÜKRÉBEN

Absztrakt

Értékelő elemzésemben a Magyar Köztársaság Alkotmányának, az Országgyűlés 94/1998-as (XII.29.) határozatának a Magyar Köztársaság biztonság és védelempolitikájának alapelveiről, a Magyar Köztársaság Nemzeti Biztonsági Stratégiájának, valamint a Magyar Köztársaság Katonai Stratégiájának az átfogó elemzése alapján összefüggéseket szeretnék felvázolni a biztonság, a Magyar Köztársaság biztonsága és a Magyar Honvédség szerepvállalása kapcsán. A teljesség igénye nélkül értelmezni szeretném a biztonság komplex fogalmát, megjelenését az érintett dokumentumokban.

In my evaluative analysis I would like to publish associations or relationships concerning security, security of the Hungarian Republic and role of the Hungarian Defence Forces on the basis of a comprehensive analysis of the Constitution of the Hungarian Republic, the 94/1998 governmental decision (The basic principle of the security and defence policy of the Hungarian Republic) and The Military and National Security Strategy of Hungary. Without need of completeness, I wish to clarify the complex concept of security and its appearance in the mentioned documents.

Kulcsszavak: *biztonság, alkotmány, biztonság és védelempolitika, katonai stratégia, euro-atlanti régió, új típusú kihívások ~ security, constitution, security and defence policy, military strategy, Euro-Atlantic region, new types of challenges*

ELŐSZÓ

A világ, amelyben élünk egy globalizált világ, melyet a különböző politikai, gazdasági, katonai szövetségesi rendszerek formálódása és léte hat át. Ebben a globalizált és szövetségesi rendszerek létezésén nyugvó világban, a biztonságnak, mint értéknek, és mint érdeknek a súlya jelentős mértékben felértékelődik. A folyamatosan változó globális viszonyok következtében azonban a biztonság komplex fogalma új értelmet nyer, új elemekkel bővül. A biztonságot veszélyeztető kockázati tényezők tárházában a klasszikus értelemben vett háborúk, az erőszak, a nukleáris fenyegetettség mellett olyan új típusú kihívások is megjelennek, mint a terrorizmus, az etnikai villongások, a regionális vagy vallási konfliktusok, az információs hadviselés [1] [2] [3], a kritikus infrastruktúra védelme [4], az illegális migráció [5], a klímaváltozás, az energiabiztonság. Ennek következtében az ország védelmét nemzeti és nemzetközi színtéren, a különböző szövetségesi rendszerek égisze alatt megtestesítő Magyar Honvédség alaprendeltetéséből és szövetségesi kötelezettségéből adódó feladatköre is átértelmeződik, újabb elemekkel bővül, összhangban a Magyar Köztársaság és a különböző szövetségesi rendszerek biztonsági értékeivel és érdekeivel.

BIZTONSÁG

A biztonság szó a latin securitas, -atis (f) szóból ered, mely többek között gond nélküli, gondtalan, biztonságos jelentéssel bír. A Hadtudományi Lexikon megfogalmazásában a biztonság nem jelent mást, mint az „… egyéneknek, csoportoknak, országoknak, régióknak, szövetségesi rendszereknek a maguk reális képességein és más hatalmak, nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete és annak tudati tükröződése, amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak az ellene való eredményes védekezés feltételei.” [6]

A biztonság egy komplex fogalom, melynek magyarázatára, kategorizálására a szakirodalomban számos megfogalmazás található. A vonatkozó magyarázatokból nyilvánvalóvá válik, hogy a fogalom tartalma vitatott, nincs egységes értelmezése, az idők folyamán folyamatosan változott, átalakult, új elemekkel bővült. Nem lehet leszűkíteni csupán a katonai jellegű fenyegetésekre és az azokra adott válaszokra.

A hidegháború időszakában a legfontosabb biztonsági kihívás, elsőrendű kockázati tényező a nukleáris háború elkerülése, a Szovjetunió térnyerésének, expanziós politikájának a megakadályozása volt. Ezt követően, az egykori szuperhatalom széthullásával, a bipoláris világrend megszűnésével és olyan új kihívásokkal kellett és kell szembenézni, mint a terrorizmus, az etnikai feszültségek, a regionális vagy vallási konfliktusok, az információs hadviselés, a kritikus infrastruktúra védelme, az illegális migráció, a klímaváltozás, az energiabiztonság. Ebből adódóan a hidegháború lezárulásával megnőtt az igény a biztonság fogalma értelmének kiszélesítésére. Ennek a törekvésnek az egyik kiemelkedő képviselője Barry Buzan híres angol politológus. Az ő megfogalmazása alapján „… a biztonság a túlélés és a fennmaradás lehetősége és képessége a létet fenyegető veszélyekkel szemben.” [7] Többek között ő tett kísérletet elsőként a biztonság különböző kategóriáinak megkülönböztetésére. Munkássága eredményeképpen a biztonság öt fő szektorát különítette el, melyek a katonai, politikai, gazdasági, társadalmi és környezeti szektorok. [8] A Hadtudományi Lexikon megfogalmazásában is megtalálhatóak ezek az alapvető szektorok, kiegészülve a humanitárius, a környezetvédelmi és a katasztrófa-elhárítási szektorokkal. [6]

A katonai szektorban jelentkező biztonsági kihívások lényege egyrészt továbbra is abban áll, hogy az egyes nemzetállamok legfőbb célja a területüknek és a lakosságuknak a védelme. Másrészt az új típusú kihívások megjelenése is jelentős feladatokat helyez erre a szektorra, gondoljunk például a terrorizmusra, mely elleni küzdelem során, az egyes nemzetállamok katonai lépésekkel reagálnak, és katonai előkészülteket tesznek a védekezés érdekében. Az új típusú kihívások velejárója a hadügyben már korábban is uralkodó aszimmetria ismételt megjelenése, melynek szereplői eltérő erejű és szintű „szembenálló felek”. Az aszimmetria elsősorban a hálózat alapú hadviselésben teljesedik ki, amikor is a konfliktus, a konfrontáció az összetett, globális méretű társadalmi, gazdasági, politikai hálózatok miatt túlnyúlik a nemzetállamok határain, így ezen okból kifolyólag nehéz felvenni ellene a küzdelmet. Jó példa erre többek között az Egyesült Államoknak a terrorizmus ellen folytatott küzdelme. [8]

A biztonsági kihívások politikai szektorának lényege az instabil államszerkezettel, társadalmi berendezkedéssel, politikai és gazdasági helyzettel rendelkező, etnikai feszültségekkel terhelt államok problematikájában nyilvánul meg. Ezekben az úgynevezett „bukott államokban” nincs egy stabil politikai kormányzás, melynek hiányában a gazdasági és a társadalmi szektorok is sérülnek. Ezek együttes hatása, pedig ellehetetleníti a fenntartható politikai, gazdasági és társadalmi fejlődést. [9] Mivel az ilyen problémákkal küszködő államok jól meghatározható földrajzi régiókban helyezkednek el, így a jelentkező nehézségek a globalizáció, a kölcsönös függőségi viszonyok, illetve a szövetségesi rendszerek miatt könnyen globális szinten jelentkezhetnek. Lokális szinten pedig

kedvezhetnek az új típusú biztonsági kihívásoknak, utalván többek között Afganisztánra, mely hasonló nehézségek miatt a terrorizmus melegágya lett. [8]

A biztonság gazdasági szektorának vonatkozásában, többek között a napjainkban meghatározó jelentőségű energiafüggőségre, az energiahordozókért folyatott küzdelemre, a gazdaság működésében rejlő problémákra és viszonyokra kell gondolni, mely a biztonságra alapvetően hatást gyakorló gazdasági stabilitás alapja. Ez a szektor szoros összefüggésben van a politikai szektorral, hiszen az instabil államok politikai rendszerének összeomlása könnyen magával hozhatja a gazdasági rendszerük megroppanását is. Ugyanakkor nagyon sok esetben ezek az úgynevezett „működésképtelen államok" jelentős volumenű nyersanyag és erőforráskészletekkel rendelkeznek. A fentiekben említett komplex függőségi viszonyok miatt a biztonság gazdasági szektorában lokális szinten megjelenő kihívások nagyon könnyen átgyűrűzhetnek globális szintre. [8]

A társadalmi szektorban rejlő kihívások okait az instabil, gyenge állami intézményekben, az etnikai és nemzetiségi ellentétekben, a társadalmi megosztottság okozta belső társadalmi problémákban találhatjuk meg. A feszültségek elsősorban a különböző csoportok közötti politikai, gazdasági hatalom megszerzéséért folytatott harcban nyilvánulhatnak meg. Az államnak nagyon fontos szerepe van a társadalmi biztonság megteremtésében az igazságos társadalmi viszonyok, a békés társadalmi léthez szükséges javak – közbiztonság, egészségügyi ellátás, honvédelem, oktatás – biztosítása által. A biztonság társadalmi szektorának globális hatásai többek között az etnikai üldöztetés, népirtás okozta tömeges migrációban, a lokális konfliktusuk eszkalálódásában [6] és a járványok terjedésében nyilvánulhatnak meg. A politikai, gazdasági szektorban rejlő kihívásokhoz hasonlóan a biztonság e szektorának instabilitása is kedvezhet a különböző szélsőséges csoportok térnyerésének. [8]

A környezeti szektorban rejlő kihívásokat górcső alá véve megállapíthatjuk, hogy alapvetően az emberi tevékenységek természeti környezetre gyakorolt hatásában keresendő a probléma oka. E szektor sajátosságaiból adódóan a felmerülő problémák – úgy, mint a napjaikban egyre inkább égetőbb túlnépesedési probléma vagy a globális felmelegedés okozta klímaváltozás - alapvetően globális szinten jelentkeznek, melyeknek rendezésében az egyes államoknak, de minden embernek, is jelentős feladata van. A környezeti szektorban rejlő problémák hatására könnyen fegyveres konfliktusok alakulhatnak ki a megújuló erőforrásokért (pl. a vízért), emellett szükséges olyan jelenségekkel is számolni, mint a vízhiány okozta migráció. Megemlítendő, hogy a fenti folyamatok következtében tovább fokozódhatnak a korábban említett „működésképtelen államok" instabilitásából származó veszélyek is. [8]

A MAGYAR KÖZTÁRSASÁG ALKOTMÁNYA [10]

Az Alkotmány a Magyar Köztársaság alaptörvénye és egyben legmagasabb szintű törvénye, a jogforrási rendszer csúcsa, melyet különleges eljárási rendben alkotnak meg. A benne foglalt alapjogok és az alkotmányos rend védelméről az Alkotmánybíróság gondoskodik. Az állam ebben szabályozza többek között a saját jogrendjét, az állampolgárok alapvető jogait és kötelezettségeit, valamint meghatározza az államszervezetre vonatkozó alapvető szabályokat. A jelenleg hatályos Alkotmány eredeti szövegét az 1949. évi XX. törvénnyel fogadta el az Országgyűlés 1949. augusztus 18-án, mely törvény 1949. augusztus 20-án lépett hatályba. Az azóta eltelt időszakban több módosításon esett át többek között a rendszerváltás, a NATO-hoz vagy az Európai Unióhoz való csatlakozásunk eredményeképpen.

A biztonság, mint fogalom, a Magyar Köztársaság biztonsága, illetve a Magyar Honvédség szerepvállalása szempontjából:

- az Alkotmány I. fejezet – Általános rendelkezések;
- II. fejezet – Az Országgyűlés;
- III. fejezet – A köztársasági elnök;
- VII. fejezet – A Kormány, VIII. fejezet – A Magyar Honvédség és egyes rendvédelmi szervek;
- valamint a XII. fejezet – Alapvető jogok és kötelességek, bír különös jelentőséggel.

Az I. fejezetben foglaltak alapján a biztonság elsődleges megtestesítője maga az állam, amely garantálja a Magyar Köztársaság és állampolgárai szabadságát, függetlenségét, az ország területi épségét, a nemzetközi szerződésekben rögzített határait a háborút kerülve és az erőszakos eszközök alkalmazását mellőzve. Ezzel párhuzamosan részt vesz az európai egység megteremtésével kapcsolatos feladatok végrehajtásában is.

A II. fejezet összhangban az első fejezettel az állami rend stabilitásának megteremtésével, az Országgyűlés vonatkozó feladataival kapcsolatos. Ezen kívül a fejezet intézkedik a Honvédelmi Tanács bizonyos speciális helyzetekben történő létrehozásáról is különböző minősített időszakokban. Ezek a minősített időszakok a rendkívüli állapot [11], a szükségállapot [11] és a hadiállapot. [6] Ebben a fejezetben már a Magyar Honvédség is megemlítésre kerül a nemzeti vagy nemzetközi alkalmazásának és szerepvállalásának vonatkozásában, mellyel kapcsolatos döntés az Országgyűlés és a Honvédelmi Tanács hatáskörébe tartozik.

A III. fejezetnek alapvetően a Magyar Honvédség vezetése szempontjából van jelentősége, melyből egyértelműen kiderül, hogy a Magyar Honvédség főparancsnoka a köztársasági elnök.

A VII. fejezet az ország és az állampolgárok biztonságának megteremtésével kapcsolatos kormányzati szintű feladatokról intézkedik. Ezek közé az alkotmányos rend védelme, a Magyar Honvédség irányítása, az élet és vagyonbiztonságot veszélyeztető vészhelyzetek [11] elhárítása, a közrend és a közbiztonság megteremtése is tartozik.

A VIII. fejezet különös jelentőséggel bír. Az alkotmány itt részletezi a Magyar Honvédség rendeltetését, alapvető feladatrendszerét nemzeti és nemzetközi szinten egyaránt, meghatározva azokat az állami szereplőket, akik az irányításában és vezetésében részt vesznek. Ennek értelmében elsődleges és legfontosabb feladata a haza katonai védelme, valamint nemzetközi szerződésekből eredő kollektív védelmi feladatok ellátása az Országgyűlés, a köztársasági elnök, a Honvédelmi Tanács, a Kormány és az illetékes miniszter irányítása alatt.

A XII. fejezet szól az állampolgároknak a biztonság megteremtésével kapcsolatos kötelezettségeiről, amelynek értelmében a haza védelmét minden állampolgár kötelességének tekinti, többek között a hadkötelezettség keretein belül.

Az Alkotmány tehát a fent említett fejezetekben írja elő az állam, a nemzeti vagyon, a nemzeti értékek, az állampolgárok egészének vagy jelentős részének a biztonságát, a vagyonbiztonságot fenyegető helyzeteknek, állapotoknak és kockázatoknak a kezelését. Állami szintű feladatokat határoz meg a veszély, a veszélyeztetettség esetére, vagyis a minősített időszakok alkalmával. Előírja a felelős személyek és szervezetek Alkotmányban rögzített feladatait az adott feltételek fennállása estén. Ezek a feladatok többek között:

- a kialakult helyzet minősítése, annak kihirdetése;
- a minősített időszakkal kapcsolatos feladatok meghatározása;
- a szükséges rendszabályok bevezetése;
- az állami élet rendjének a szabályozása,
- valamint az állampolgárok igénybevételének az elrendelése.

Meglátásom szerint az Alkotmányban rögzített ide vonatkozó dolgok szorosan összekapcsolhatóak a biztonság katonai, társadalmi és politikai szektorával, mivel elítél minden olyan erőszakos cselekedetet, amely a hatalom megszerzése által egy instabil államszerkezetet, politikai intézményrendszert és társadalmi berendezkedést idézne elő. A globális biztonság szellemében pedig célul tűzi ki az európai egység megteremtését.

AZ ORSZÁGGYŰLÉS 94/1998-AS (XII.29.) HATÁROZATA A MAGYAR KÖZTÁRSASÁG BIZTONSÁG ÉS VÉDELEMPOLITIKÁJÁNAK ALAPELVEIRŐL [12]

A Magyar Köztársaság biztonságpolitikáját meghatározó egyik legfontosabb jogi dokumentum az országgyűlés 94/1998-as (XII. 29.) határozata, mely hatálytalanította a 11/1993. (III.12.) évi országgyűlési határozatot, valamint a 27/1993. évi (IV.23.) országgyűlési határozatot. Ezek közül az előbbi a Magyar Köztársaság biztonságpolitikai, míg az utóbbi a honvédelmi alapelveiről szólt. Mint azt korábban az Alkotmánnyal kapcsolatos módosítások tekintetében is említettem, a globalizálódó világ, a megszülető szövetségesi rendszerek, hazánk NATO- és EU tagsága eredményezték ennek a két korábbi határozatnak is a hatálytalanítását, és a nevezett országgyűlési határozat megszületését.

A 94/1998-as országgyűlési határozat a Magyar Köztársaság biztonság- és védelempolitikai alapelveit fogalmazza meg. Az elvek felsorakoztatása során egyértelműen utal arra, hogy a Magyar Köztársaság a biztonságot - a már korábban említettek szerint - komplexitása alapján értelmezi. Ez az olvasat a hagyományos értelemben vett politikai és katonai szektoron túlmenően magába foglalja többek között a gazdasági, pénzügyi, emberi jogi és kisebbségi, információs és technológiai, környezeti és a nemzetközi jogi szektorokat is, és ugyancsak utal a biztonságot veszélyeztető kockázati tényezők kiszélesedett spektrumára. Ebben az aspektusban a biztonságra ható veszélyforrásokat alapvetően

globális:
- terrorizmus;
- szervezett bűnözés;
- illegális migráció;
- gazdasági válságok;
- pénzügyi válságok;
- társadalmi válságok;
- tömegpusztító fegyverek,
- környezeti ártalmak;
- információs hadviselés;

regionális:
- a demokratizálódási folyamatok törékenysége;
- instabilitás és kiszámíthatatlanság;
- a nemzeti kisebbségek jogainak háttérbe szorítása;

és lokális szinten:
- a piacgazdaság kialakulását gátló tényezők;
- a gazdasági növekedés, jólét és az életminőség javulása ellen ható tényezők alapján különíti el.

A dokumentum megfogalmazza az ország biztonságpolitikájának legfőbb céljait, - melyek szoros összhangban állnak az Alkotmány szövegével – úgy, mint:

- az ország függetlenségének, szuverenitásának, területi épségének a szavatolását;
- az alkotmányos rend, a demokratikus jogállamiság, a piacgazdaság kedvező feltételeinek a megteremtését;
- a különböző emberi jogok érvényesülésének a biztosítását;
- az élet, vagyon és szociális biztonság megteremtését;
- a nemzetközi béke és biztonság fenntartását;
- az euro-atlanti régió stabilitását;
- az ország kedvező és stabil nemzetközi gazdasági, politikai és kulturális kapcsolatainak a megteremtését és fenntartását.

Az országgyűlési határozat utal arra, hogy a fent említett biztonságpolitikai célkitűzéseket a Magyar Köztársaság milyen módon kívánja megvalósítani. Ennek értelmében kimondja, hogy a biztonságpolitikai elképzeléseit az Alkotmánnyal összhangban, a különböző nemzetközi szervezetek, mint az ENSZ [13], az EBESZ [14] [15], az Európa Tanács [16], az Észak-atlanti Szerződés Szervezete [17] [18] dokumentumaiban rögzített alapelveknek és kötelezettségvállasoknak megfelelően kívánja megvalósítani. A biztonság szempontjából tesz egy nagyon fontos megállapítást, - eszerint kimondja, hogy az országnak nincsen ellenségképe, a nemzetközi jog előírásait betartó nemzetközi színtér szereplőit partnerként kezeli, a vitás kérdéseket pedig a nemzetközi jog előírásait figyelembe véve békés eszközökkel kívánja rendezni.

Az országgyűlési határozatból nyilvánvalóvá válik, hogy az ország, azonosul a globalizálódó, szövetségesi rendszereken nyugvó világ kihívásaival. Az állampolgárainak a biztonságát ebben a környezetben, az euroatlanti régió szerves részeként, a NATO égisze alatt fennálló kollektív védelmen alapulva képzeli el garantálni.

Az országgyűlési határozat kötelezettséget vállal arra, hogy megteremti a benne foglalt feladatok végrehajtásához szükséges feltételeket, és felelőssé teszi a Kormányt a Nemzeti Biztonsági Stratégia és a Nemzeti Katonai Stratégia kidolgozásáért, felülvizsgálatáért, valamint a bennük meghatározott feladatok végrehajtásáért.

A fentieket összegezve levonható az a következtetés, hogy az országgyűlési határozat megszületése többek között a globalizálódó világ, a változó szövetségesi rendszerek, az új típusú kihívások megszületésének az eredménye. A Magyarország biztonságának megteremtésével kapcsolatos feladatok és intézkedések során figyelembe veszi a biztonság fogalmának komplexitását és mindazokat a globális, regionális és lokális veszélyforrásokat, melyek a biztonság fenntartására vagy megteremtésére közvetlen hatást gyakorolnak. A Magyar Köztársaság biztonságának megteremtését a kollektív védelem keretében, a nemzetközi szövetségesi rendszerek égisze alatt kívánja megvalósítani.

A MAGYAR KÖZTÁRSASÁG NEMZETI BIZTONSÁGI STRATÉGIÁJA [19]

A Magyar Köztársaság Nemzeti Biztonsági Stratégiáját 2004. március 31-e ülésén fogadta el a Kormány a 2073/2004 (III.31.) kormányhatározat formájában. A határozat 2004. április 15-én lépett hatályba felváltva ez által a korábban érvényben lévő 2144/2002 (V.6.) kormányhatározatot a Magyar Köztársaság Nemzeti Biztonsági Stratégiájáról. A korábbi stratégia átdolgozását ebben az esetben is a globális változások indokolták, melyek során az európai integrációs folyamat egyik jelentős mérföldköveként 2004. május 1-vel Magyarország az Európai Unió teljes jogú tagja lett.

A stratégia a Magyar Köztársaság biztonság és védelempolitikai alapelveire épít összhangban a NATO 1999. évi Stratégiai Koncepciójával [20], valamint az Európai Unió

által 2003-ban elfogadott Európai Biztonsági Stratégiával. [21] A kormányhatározat alapvetően:

- a biztonsággal kapcsolatos értékek és érdekek;
- a biztonsági környezet (fenyegetések, kockázatok, kihívások);
- az elérendő célok és a végrehajtandó feladatok;
- a megvalósításhoz szükséges eszközök;
- valamint az ágazati stratégiák:
    - katonai;
    - nemzetbiztonsági;
    - rendvédelmi;
    - gazdasági-pénzügyi;
    - humánerőforrás-fejlesztési;
    - szociálpolitikai;
    - informatikai és információvédelmi;
    - katasztrófavédelmi és környezetbiztonsági;
    - terrorizmus elleni küzdelem kérdéskörével foglalkozik.

A Nemzeti Biztonsági Stratégia megfogalmazásában a Magyar Köztársaság a biztonságot, mint alapvető értéket kezeli:

- a béke;
- a stabilitás;
- a szuverenitás;
- a demokrácia;
- a jogállamiság;
- a vállalkozás szabadsága;
- az emberi és az alapvető szabadságjogok tiszteletben tartása;
- valamint a magyarság kulturális örökségének és identitásának megőrzése mellett.

Ezeknek az értékeknek a védelme, létük stabilitásának a megteremtése meghatározó jelentőséggel bír a korábban említett biztonsági szektorok kapcsán is.

A biztonsággal kapcsolatos érdekek közé sorolja többek között:

- az ország területének, szuverenitásának, alkotmányos rendjének megőrzését;
- a nemzetközi béke és biztonság fenntartását;
- az Európai Unió integrációjának és a közös európai politikának kiterjesztését;
- a nemzetközi béke és biztonság erősítését;
- a fenntartható gazdasági növekedést;
- az állampolgárok biztonságának és jólétének az előremozdítását;
- valamint az euro-atlanti térség stabilitásának megőrzését.

A fentieket tekintve megállapítható, hogy szinte teljes az összhang az Alkotmányban és a 94/1998-as országgyűlési határozatban rögzített biztonságpolitikai célkitűzésekkel.

A biztonsági környezet, az arra hatást gyakorló fenyegetések, kockázatok és kihívások vonatkozásában - hasonlóan a 94/1998-as országgyűlési határozathoz - megkülönbözteti a kockázati tényezők globális, regionális és lokális dimenzióját. Ennek következtében a globális dimenzió keretében:

- a terrorizmusban;
- a fegyverkereskedelemben;

- a tömegpusztító fegyverekben;
- az illegális migrációban;
- valamint az információs hadviselésben rejlő, a biztonságot veszélyeztető kihívások jelennek meg.

Regionális szinten olyan fenyegetésekről esik szó, mint:

- a Közép-Európában és Délkelet-Európában (társadalmi, szociális ellentmondások, nemzeti, etnikai, kisebbségi és vallási problémák);
- a FÁK- országokban (bűnözés, illegális migráció, terrorizmus);
- a mediterrán térségben (szegénység, gyors népességnövekedés, migráció, terrorizmus, szervezett bűnözés);
- valamint a Közel- és Közép-Kelet (vallási, politikai, területi viták, terrorizmus, tömegpusztító fegyverek, energiahordozók ellenőrzésére irányuló törekvések) gócpontjaiban rejlő veszélyforrások.

A belső kihívásokat tekintve a legfőbb kockázati tényezők között említi a dokumentum:

- a szervezett bűnözést;
- a feketegazdaságot;
- a korrupciót;
- a kábítószerek terjedését;
- a politikai és vallási szélsőségek megerősödését;
- valamint a demográfiai kihívásokat.

A szövetségesi kötelezettségekkel párhuzamosan a dokumentum a saját képességek fejlesztésére is jelentős hangsúlyt fektet. Az elérendő célok között jelöli a nemzetközi szervezetekhez, mint:

- a NATO-hoz (a hagyományos védelmi feladatok, a szövetségesi együttműködés képességeinek megőrzése, az euroatlanti régióban és azon kívül jelentkező válságkezelés);
- az Európai Unióhoz (részvétel az Európai Unió közös kül és biztonságpolitikájában, gazdaságpolitikai integráció elmélyítése);
- a transzatlanti együttműködés területéhez (terrorizmus elleni küzdelem, NATO és Európai Unió stratégiai partnerség elmélyítése);
- az ENSZ-hez (részvétel a békefenntartó missziókban, hozzájárulás a világszervezet alkalmazkodásához az új típusú kihívásokhoz);
- az EBESZ-hez (részvétel EBESZ-missziókban, a fegyverzetellenőrzésben);
- valamint a gazdasági diplomácia területéhez kapcsolódó célkitűzéseket (tagságunk fejlesztése a regionális gazdasági szervezetekben).

Megfogalmazza továbbá a térségünk államaival való kapcsolattartás fontosságát, melynek értelmében a kétoldalú és regionális kapcsolatok terén, a határon túli magyarok vonatkozásában és a FÁK-országokkal kapcsolatban jelöl meg feladatokat.

A globális térben jelentkező fenyegetésekhez és kihívásokhoz fűződő célkitűzések:

- a terrorizmus és a tömegpusztító fegyverek alkalmazásának megakadályozása elleni küzdelemben;
- a regionális konfliktusok kezelésében;
- az államépítésben;

- a humanitárius segítségnyújtásban;
- a schengeni együttműködésben;
- az információs rendszerek védelmében;
- a természeti és civilizációs környezet védelmében testesülnek meg.

A belső kihívásokkal kapcsolatos legfontosabb biztonságot elősegítő és fokozó célkitűzések:

- a szervezett bűnözés;
- a feketegazdaság;
- a korrupció;
- a kábítószerek terjedése;
- a politikai és vallási szélsőségek elleni küzdelemben;
- és a demográfiai kihívásokra adott válaszokban érhetőek tetten.

A stratégia soron következő fontos része a nemzeti biztonsági stratégia megvalósításához szükséges eszközöket sorolja fel, melyek között legfontosabbaknak:

- a feltételeket biztosító nemzetgazdaságot;
- a hazai és a nemzetközi élet minden területén megnyilvánuló együttműködést;
- a megfelelő politikai, diplomáciai, katonai, katasztrófa-elhárítási területeket jelöli meg, melyek az ágazati stratégiák legfontosabb alappillérei.

Erre a gondolatra épül a dokumentum utolsó része, mely egyértelművé teszi, hogy a biztonság realizálásával kapcsolatos feladatok megoszlanak a különböző ágazatok között - ebből adódóan minden ágazat számára előírja, hogy dolgozza ki a saját szakterületére vonatkozó, a Magyar Köztársaság külső és belső biztonságának fenntartásához kapcsolódó gyakorlati módozatokat, stratégiákat -.

Konklúzióként megállapítható, hogy a Nemzeti Biztonsági Stratégia eleget tesz az országgyűlési határozatban foglalt kötelezettségeknek. A Kormány egy olyan stratégiát dolgozott ki, mely megfelel a kor kihívásainak, elvárásainak. A dokumentum reális értékelése a világban végbement változásoknak, a végrehajtandó feladatokat és az azok megvalósításához szükséges célokat ennek szellemében fogalmazza meg, és alakítja ki, továbbá igyekszik választ adni a biztonság valamennyi szektorában felmerülő kihívásokra.

A MAGYAR KÖZTÁRSASÁG KATONAI STRATÉGIÁJA [22]

A Magyar Köztársaság Nemzeti Katonai Stratégiáját 2009. január 30-án fogadta el a kormány az 1009/2009 (I.30.) kormányhatározat formájában, mely 2009. február 05-én lépett hatályba. Mint már korábban is említettem, ebben az esetben is igaz, hogy a nevezett katonai stratégia kidolgozását is a folyamatosan változó biztonsági környezet ihlette. Markánsan tükröződik benne a biztonsággal kapcsolatban már oly sokszor említett új felfogás, valamint az új típusú kihívásokra való reagálás.

A katonai stratégia taglalja a Magyar Köztársaság megváltozott biztonsági környezetét, védelempolitikájának alappilléreit, a Magyar Honvédség feladatait, alkalmazásának várható körülményeit, szükséges képességeit, a haderő-fejlesztési irányokat, valamint a Honvédség fenntartásának és fejlesztésének feltételeit.

A megváltozott biztonsági környezettel kapcsolatban említést tesz a globalizálódó világról, melynek következtében az átfogó biztonság keretében nem választható el egymástól a közvetlen környezet, a régió, a kontinens és a távolabbi területek biztonsága. A biztonság

megteremtésében kulcsfontosságú szerepet játszanak azok a nemzetközi szervezetek (NATO, EU), melyekbe hazánk integrálódott. Ennek a folyamatnak az eredményeképpen az ország biztonsági helyzete egyre stabilabb, de mindezek mellett a globális folyamatok következtében ezt a biztonságot egyre távolabbi régiók és újabbnál újabb kihívások veszélyeztethetik. A dokumentum a potenciális veszélyforrások között nevezi meg:

- a terrorizmust;
- a tömegpusztító fegyverek alkalmazásának elterjedését;
- a kábítószer kereskedelmet;
- a klímaváltozást;
- és az olyan kedvezőtlen demográfiai változásokat, mint a túlnépesedést, a politikai és vallási szélsőségek felerősödését.

A Magyar Köztársaság védelempolitikai alapelveit tekintve a honvédelem két legfontosabb alappillérének a nemzeti haderőt és a szövetségen belüli együttműködést tekinti. A korábbi Nemzeti Biztonsági Stratégiában foglaltakhoz hasonlóan kihangsúlyozza, hogy Magyarországnak nincsen ellenségképe, hazánk a NATO, az EU, az ENSZ, valamint az EBESZ konstruktív és aktív tagja kíván lenni. Ennek érdekében a Magyar Honvédség a lehetőségeihez mérten részt vállal, és részt kíván vállalni a régió és a világ stabilitásának megőrzését szolgáló békefenntartó és humanitárius műveletekben.

A biztonság dimenzióinál a hagyományos értelemben vett politikai és katonai dimenziókon túl, annak:

- gazdasági;
- pénzügyi;
- energiaellátási;
- rendvédelmi;
- emberi jogi és kisebbségi;
- információs és technológia;
- környezeti;
- demográfiai;
- civilizációs;
- egészségügyi;
- és nemzetközi jogi dimenzióival is számol.

A Magyar Honvédségre háruló jövőbeni feladatok és azok végrehajtási környezetével kapcsolatban megfogalmazódik a dokumentumban, hogy továbbra is a Magyar Köztársaság védelme, a NATO kollektív védelméből adódó feladatok és a nemzetközi műveletekben való részvétel kap nagy hangsúlyt. Ezek keretében olyan konkrét feladatokról van szó többek között, mint az ország függetlenségének, területi épségének a szavatolása, a befogadó nemzeti támogatás és a hatékony légtérvédelem. A dokumentum szerint az országnak továbbá olyan új típusú feladatokkal is számolnia kell, mint az illegális migráció, az elhúzódó konfliktusok, a terrorizmus, az aszimmetrikus konfliktusok kezelése és a tömegpusztító fegyverek alkalmazásával szembeni hatékony védekezés.

A dokumentum a megváltozott biztonsági környezettel és az új típusú kockázati tényezőkkel összhangban megfogalmazza az egyes elérendő célokat a haderőfejlesztés és a még hiányzó képességek tekintetében. Ezek alapján természetesen nagy hangsúlyt kell helyezni a NATO és EU képességek fejlesztésére mind a szárazföldi erő mind pedig a légierő vonatkozásában. A haderőfejlesztésnek képességalapúnak kell lennie, mely lehetővé teszi a hatékony reagálást a megváltozott globális viszonyokra. Ezek sarokkövei:

- a tábori híradó és informatikai rendszerek rendszerszemléletű fejlesztése;
- a hálózatalapú működés kialakítása;
- a szárazföldi erő mobilitásának, tűzerejének és védettségének növelése;
- a légierő modernizációja, kapacitásának növelése;
- a katonák egyéni felszerelésének korszerűsítése;
- valamint a technikai felderítő eszközök rendszerbe állítása.

Természetesen a megjelölt képességek és haderő-fejlesztési irányok eredményes megvalósítása elképzelhetetlen állami közreműködés nélkül. Itt a civil erőforrásoknak az ország védelmébe történő bevonásáról, a szükséges jogi és technikai infrastruktúra kialakításáról van szó. Ezek alapján megállapítható, hogy a jövőbeni stabil, hatékony és rugalmas haderővel szemben támasztott legfontosabb követelmények:

- a stratégiai környezet változásaihoz való alkalmazkodás képessége;
- a gyorsan változó harcászati, hadműveleti helyzetre való reagálás képessége;
- az erők megfelelő készenléti kategóriákban való tartása;
- a többnemzeti összhaderőnemi környezetben való tevékenység;
- az interoperabilitás;
- a harc hatékony megvívása;
- az erők védelme és megóvása;
- a hálózatközpontú környezetben való alkalmazás képessége;
- a hatékony felderítés és információszerzés;
- a telepíthetőség és a mobilitás;
- valamint képesség a lakossággal és a civil környezettel való együttműködésre.

A katonai stratégia utolsó részében a Magyar Honvédség fenntartásának és fejlesztésének feltételeit taglalja, melyben nagy hangsúlyt helyez annak alapvető és legfontosabb alkotóelemére, a katonára. Ebből kifolyólag különös figyelmet kell fordítani a személyi állomány megtartására, kiszámítható jövőképének a kialakítására, megfelelő kvalitásaira, kiképzésére és felkészítésére. A dokumentumban megfogalmazódik, hogy a hatékony védelem és biztonság garantálása érdekében nélkülözhetetlen a szükséges anyagi és pénzügyi források megteremtése, biztosítása, a védelmi kiadások tervszerű növelése és a Védelmi Tervezési Rendszer hatékony működtetése és fejlesztése. Ezekkel együtt kiemeli a stratégiai tartalékok képzését, a haditechnikai eszközök, a készletekkel való gazdálkodás elveinek és a honvédelmi infrastruktúrának a fejlesztését is.

Véleményem szerint a fentiek alapján megállapítható, hogy a katonai stratégia eleget tesz a 94/1998-as kormányhatározat kívánalmainak. A megváltozott biztonság és biztonsági környezet kihívásaira adandó válaszok mellett megnevezi az azok megadásához szükséges feltételeket is. Konkrét iránymutatást fogalmaz meg egy ütőképes, az adott kor színvonalának megfelelő, a megváltozott biztonsági kihívásokra hatékonyan és rugalmasan reagálni képes haderő felépítésével és továbbfejlesztésével kapcsolatban.

KONKLUZIÓ

Az érintett dokumentumok elemzése alapján elmondható, hogy az azokban foglalt alapelvek, feladatok és iránymutatások figyelembe veszik a megváltozott kor követelményeit a biztonsággal, a Magyar Köztársaság biztonságának értelmezésével, megteremtésével és a Magyar Honvédség alkalmazásával kapcsolatban. Túllépve a hagyományos értelemben vett biztonság fogalmán, azt átfogó, komplex és globális módon kezelik.

Véleményem szerint a szövetségesi tagság és a nemzetközi integráció elkötelezett híveként a Magyar Köztársaság a biztonságpolitikai célkitűzéseit és a megteremtésükhöz szükséges feltételrendszert összhangba kívánja hozni a nemzetközi előírásokkal és elvárásokkal oly módon, hogy hatékonyan reagálni tudjon a megváltozott kihívásokra, a korunkban jellemző új típusú veszélyforrásokra. A nemzetközi integrációs folyamatban állampolgárainak a biztonságát békés eszközökkel kívánja szavatolni, partnerként kezelve a nemzetközi integráció résztvevőit. A biztonság szavatolása egyik sarokkövének a kollektív védelmet tekinti, de mindezek mellett figyelmet fordít a saját képességek fejlesztésére is.

Az elemzett dokumentumok nem csak fogalmi magyarázatokkal, elvi felvetésekkel szolgálnak a komplex biztonságról, hanem konkrét célokat, feladatokat, iránymutatásokat fogalmaznak meg az azt veszélyeztető kihívásokra adandó válasszal kapcsolatban is. Megjelölik a Magyar Honvédség, mint a Magyar Köztársaság biztonságát elsődlegesen szavatoló fegyveres szervezet jövőbeni fejlesztési irányait is, melynek eredményeképpen egy rugalmasan reagálni képes, hatékony, gazdaságos működésű, a nemzetközi elvárásoknak és a szövetségesi kötelezettségeknek eleget tevő haderő alakulhat ki.

HIVATKOZÁSOK

[1] Az információs hadviselés hazai kormányzati kihívásai. Tanulmány kivonat. – p. 1-6.(Forrás:http://www.enoadvisory.com/doc/Informacios_Hadviseles_Tanulmany_EXTRACT_ENO_Advisory.pdf /letöltés ideje: 2009.10.24./)

[2] Szabó András: Az információs hadviselés és a hadtudomány. – In: Hadtudomány A Magyar Hadtudományi Társaság folyóirata, 1998. December, VIII. évfolyam 4. szám (elektronikus). (Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/1998/ht-1998-4-5.html /letöltés ideje: 2009.10.24./)

[3] Nemzetközi Hírközlési és Informatikai Tanács - Információs Társadalom Technológia Távlatai - Körkép 2007. Szeptember Október. – p. 1-25. (Forrás: http://www.nhit-it3.hu/it3-cd/IT3_korkep_07szept_okt.pdf /letöltés ideje: 2009.10.24./)

[4] 2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. – p. 1-22. (Forrás:http://www.bm.hu/web/jog_terv.nsf/0/19659F03FD726909C12574C20034751C/$FILE/2080_2008_Korm-hat.pdf /letöltés ideje: 2009.10.23./)

[5] Glatz Ferenc: Migráció a kibővített Európai Unióban. – p. 400-407. (Forrás: http://www.glatzferenc.hu/upload/file/Kotetek/5K-50.pdf /letöltés ideje: 2009.10.24./)

[6] Magyar Hadtudományi Társaság: Hadtudományi Lexikon I. kötet. Szabó József (főszerk.) – Budapest,1995. – 144. p. – ISBN 963 04 5227 8

[7] Matus János: A biztonság és a védelem problémái a változó nemzetközi rendszerben. – In: Hadtudomány A Magyar Hadtudományi Társaság folyóirata, 2005. december, XV. évfolyam 4. szám (elektronikus). (Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_24.html /letöltés ideje: 2009.10.24.)

[8] Biztonságpolitikai szemle Corvinus Külügyi és Kulturális Egyesület. – Corvinák. – 1. A biztonsági kihívások új felfogása. - Az új típusú biztonsági kihívások új elméleti keretben. (Forrás: http://bizpol.playhold.hu/?module=corvinak&module_id=4&cid=1 /letöltés ideje: 2009.10.24./)

[9] Magyar UNESCO Bizottság – A fenntartható fejlődés fogalma, célkitűzése. (Forrás: http://www.unesco.hu/index.php?type=node&id=131 /letöltés ideje: 2009.10.27./)

[10] A Magyar Köztársaság Alkotmánya. (Forrás: http://net.jogtar.hu/jr/gen/getdoc.cgi?docid=94900020.tv /letöltés ideje: 2009.11.07./)

[11] Magyar Hadtudományi Társaság: Hadtudományi Lexikon II. kötet. Szabó József (főszerk.) – Budapest,1995. – ISBN 963 04 5228 6

[12] Az Országgyűlés 94/1998-as (XII.29.) határozata a Magyar Köztársaság biztonság és védelempolitikájának alapelveiről. (Forrás: http://www.complex.hu/kzldat/o98h0094.htm/o98h0094.htm /letöltés ideje: 2009.11.07./)

[13] Az Egyesült Nemzetek Szervezete. (Forrás: http://www.menszt.hu/ /letöltés ideje: 2009.11.07./)

[14] Európai Biztonsági és Együttműködési Szervezet. (Forrás: http://www.mfa.gov.hu/kulkepviselet/AT_EBESZ/hu/EBESZ/EBESZ.htm /letöltés ideje: 2009.11.07./)

[15] Európai Biztonsági és Együttműködési Szervezet. (Forrás: http://bizpol.playhold.hu/?module=corvinak&module_id=4&cid= /letöltés ideje: 2009.11.07./)

[16] Európa Tanács. (Forrás: http://www.europatanacs.hu/ /letöltés ideje: 2009.11.07./)

[17] Észak Atlanti Szerződés Szervezete. (Forrás: http://bizpol.playhold.hu/?module=corvinak&module_id=4&cid=107 /letöltés ideje: 2009.11.07./)

[18] Észak Atlanti Szerződés Szervezete. (Forrás: http://www.nato.int/cps/en/natolive/index.htm /letöltés ideje: 2009.11.07./)

[19] A Magyar Köztársaság Nemzeti Biztonsági Stratégiája. (Forrás: http://www.hm.gov.hu/hirek/kozlemenyek/a_magyar_koztarsasag_nemzeti_biztonsagi_strategiaja /letöltés ideje: 2009.11.07./)

[20] A NATO katonai stratégiái. (Forrás: http://bizpol.playhold.hu/?module=corvinak&module_id=4&cid=109 /letöltés ideje: 2009.11.08./)

[21] Az európai biztonság és védelempolitika kialakulásának és fejlődésének története. (Forrás:http://www.mfa.gov.hu/kum/hu/bal/Kulpolitikank/Biztonsagpolitika/esdp/eu_biztonsag_vedelempol_ebvp_tortenet.htm /letöltés ideje: 2009.11.08./)

[22] A Magyar Köztársaság Katonai Stratégiája. (Forrás: http://www.honvedelem.hu/cikk/0/13818/katonai_strategia_kormanyrendelet.html /letöltés ideje: 2009.11.08./)

Kendernay Zsolt – Pándi Erik – Jobbágy Szabolcs
kendernayz@mail.ahiv.hu – pandi.erik@zmne.hu – jobbagy.szabolcs@zmne.hu

A BEVETÉS- ÉS MENTÉSIRÁNYÍTÁSI RENDSZEREK EGYSÉGESÍTÉSÉNEK ALAPJAI, JOGI HÁTTERE[1]

Absztrakt

Jelen közlemény a hazai bevetés- és mentésirányítási rendszerek alapkérdéseivel foglalkozik.

This publication deals with fundamental questions related to national deployment - and rescue control systems.

Kulcsszavak: *bevetés-irányítás, Egységes Segélyhívó Rendszer (112) ~ deployment management, 112 Emergency System*

BEVEZETÉS

A 112-es hívószámon alapuló Egységes Segélyhívó Rendszer (ESR) rendszer kérdéskörét érintve több publikáció, tanulmány is megjelent, hiszen az Európai Unió (EU) elvárásai, a társadalmi igény és a környezeti hatások is szükségessé teszik, hogy a Tagállamok között és magukban a Tagállamokban is egységessé váljon egy olyan segélyhívó rendszer, melyet az állampolgárok szükség esetén bármikor, bárhonnan elérnek. Ennek jogi szabályozását, több törvényt, rendeletet, sőt maga az Alkotmány is tartalmazza. Az Alkotmány 70/D § biztosítja a „lehető legmagasabb szintű testi és lelki egészséghez való jogot". A törvények, rendeletek hozzájárulnak a társadalmi közszükségletet kielégítő alapvető szolgáltatás folyamatos biztosításához, baleset, elemi csapás vagy súlyos kár, továbbá egészséget, testi épséget fenyegető veszély megelőzéséhez illetőleg elhárításához, valamint az alkalmazott technológia biztonságos, rendeltetésszerű alkalmazásának fenntartásához.

Amikor katasztrófavédelemről, vészhelyzet elhárításáról beszélünk, akkor tudnunk kell, hogy ennek igen sokféle változatával találkozhatunk. Létezik például biológia (járványok, stb.), természeti (földrengés, árvíz, stb.), vegyi (nukleáris, stb.), katonai, biztonsági (terrorcselekmények, stb.) civilizációs (légszennyezés, veszélyes hulladékok, stb.). Az ezekkel összefüggő feladatok elhárításával, felszámolásával, segítségnyújtással Magyarországon több szervezet foglalkozik. Például Országos Rendőr-főkapitányság (ORFK), Országos Katasztrófavédelmi Főigazgatóság (OKF), Tűzoltóság, Országos Mentőszolgálat (OMSZ), Vám- és Pénzügyőrség Országos Parancsnoksága, Országos Környezetvédelmi, Természetvédelmi és Vízügyi Főigazgatóság, Büntetés-végrehajtás Országos Parancsnoksága, Magyar Honvédség, Nemzetbiztonsági Szolgálatok. Jelen közleményünkben a három legérintettebb szervezettel az Országos Rendőr-főkapitányság (ORFK), Országos Katasztrófavédelmi Főigazgatóság (OKF), Országos Mentőszolgálat (OMSZ), mint készenléti szervezetekkel foglalkozunk. A feladathoz szükséges szolgálatirányítás, a mentés, a bevetés személyi, operatív, technikai hátterének feltételeinek kialakítása az érintett szervezetek feladata.

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült

Munkánk célja a készenléti szervek szolgálat-, bevetés- és mentésirányítási rendszerei egységesítési kérdéseinek vizsgálata, hiszen az emberek életének, épségének, a közrend, a közszolgáltatások fenntartásának elengedhetetlen feltétele, a készenléti szervezetek együttműködésének erősítése, infokommunikációs rendszerük közös platformba vonása.

1. FOGALMAK

Ahhoz, hogy a meglévő és jövőbeli rendszerek fontosságát átlássuk, tisztáznunk kell bizonyos szavakat, fogalmakat és nagyvonalakban ismernünk kell a rendszer egyediségét, jellemzőit, céljait.

Szolgálat

Meghatározott feladatkör ellátását végző egységek, csoportok, melyet a társadalom egésze érdekében konkrét céllal működtetnek.

Bevetés

Csoportok vagy egységek meghatározott helyre küldése bizonyos feladatok elvégzése céljából.

Mentés

Veszély, kár, stb. felszámolására, kiszabadítására irányuló cselekedetek.

Készenléti szervezet

Olyan alapvető állami feladatot ellátó, bevetésre kész, azonnali cselekvésre, beavatkozásra, állapotra szerveződő egységek, csoportok, intézmények, melyek képesek a társadalmi közszükségletet kielégítő alapvető szolgáltatás folyamatos biztosítására, balesetek, elemi csapások vagy súlyos kárt, egészséget, testi épséget fenyegető veszély megelőzésére, elhárítására, illetőleg az alkalmazott technológia biztonságos, rendeltetésszerű alkalmazásának fenntartására.

Rendszer

„Általános fogalom, amely a számítástechnikában utalhat számítógépre önállóan vagy perifériákkal együtt, hálózatra, operációs rendszerre, esetleg annak egy elkülönített részére (pl. állományrendszer)”[2]

Szolgálat-, bevetés- és mentésirányítási rendszer

Olyan összetartozó adatok, funkciók, eszközök rendezett halmaza, mely kielégíti a készenléti szervezetek szolgálat-, mentés-, bevetésre irányuló tevékenységéhez szükséges technológiai igényeket, valamit adott konfigurációval hozzáférést biztosít erőforrásaihoz.

2 Forrás: Angol- magyar Informatikai értelmező szótár PANEM Budapest, 2004 263. oldal

2. SZOLGÁLAT-, BEVETÉS ÉS MENTÉSIRÁNYÍTÁSI RENDSZEREK ÉS FOLYAMATOK JELLEMZŐI

A következőkben a készenléti szervezetek (ORFK- Rendőrség, OKF, OMSZ) szolgálat, bevetés és mentésirányításra vonatkozó sajátosságait foglaltuk össze az infokommunikációs terület vetületére koncentrálva.

Párhuzamosság

Segélyhívó rendszerként több egymás mellett élő megoldás is azonosítható, hiszen egyaránt működik az európai segélyhívó vonal (112) és a hagyományosnak tekinthető nemzeti segélyhívó számok (104, 105, 107). Az állampolgárok bejelentéseiket ezeken a csatornákon tehetik meg az egyes szolgálatok, Rendőrség, Tűzoltóság, Országos Mentő Szolgálat, vagy esetleg a Katasztrófavédelem felé.

Nincs egységes segélykérés, bejelentés kezelés

A két különböző típusú bejelentési csatorna esetében más és más folyamati és technológiai megoldással futnak be az információk az érintett kapitányságokra, parancsnokságokra, mentőállomásokra.

A szolgálat-, bevetés és mentésirányítási rendszer részleges

Mindhárom szervezetnél működik valamilyen szintű rendszer, de nem elég hatékonyak, ezért a rendszerelemek funkcióinak összehangolása, bővítése szükséges.

Nincs központosított híváskezelés

A nemzeti segélyhívók használata során mindig az adott telefonszámhoz rendelt szolgálat helyi egysége felé történik a hívásátirányítás, ahol azonnali intézkedéseket tudnak megkezdeni. A hívások kezelése szervezetileg tehát nem központosított módon történik.

Azonnali végrehajtás, gyors döntés hiánya

A telefonon érkező segélyhívások esetében a társszervek értesítése és a bejelentés átadása jelenleg kézi úton történik, azaz az ügyeletes további telefonhívások lebonyolítására kényszerül. Az állampolgárok akkor tartják megfelelő színvonalúnak a szolgáltatásokat, ha nemcsak gyorsan és könnyen tudják megtenni bejelentéseiket, hanem akkor, ha a Rendőrség, a Tűzoltóság, a Mentők gyorsan és szakszerűen képesek reagálni.

Segélyhívási folyamatok nem standardizáltak

A bejelentések automatizált kezelése nem megoldott. Jelenleg az ügyeletes saját tapasztalataira és szakmai felkészültségére támaszkodva kezeli a bejelentéseket, tehát a szolgálatban lévő egységekről meglévő információi és a megfelelő intézkedési protokollok ismerete alapján hoz döntéseket. A helyi ügyeletes csak saját erőit látja nem képes allokálni más szabad egységeket.

Eszköz és informatikai rendszer hiánya

Általánosan elmondható, hogy elavult eszközparkkal (tűzoltóság, mentők) rendelkeznek, melyet az informatikai háttér hiánya csak fokoz. A feldolgozási folyamat és az érintettekkel való hatékony kapcsolattartás nehezen kivitelezhető. Az irányítás során csak korlátozott lehetőség van nyomon követni az intézkedés folyamatát (EDR kapcsolat).

Elavul, nem megfelelő átviteltechnika

A szervezetek közötti adatátviteli kommunikáció részleges és nem egységes sem szervezeti keretében, sem pedig műszaki, technikai megvalósításában. A Rendőrség saját úgynevezett zártcélú Rendészeti Hálózattal (zRH) rendelkezik, amelyet a KEK KH Adathálózati és Távközlési Főosztálya működtet. Az OMSZ gyakorlatilag nem rendelkezik átviteltechnikai megoldással, vagy ahol van, közvetlen az Elektronikus Kormányzati Gerinchálózatot (EKG) használja. Az OKF megoldási módja vegyes, ami azt jelenti, hogy van ahol EKG-t, van ahol a zRH-t használja.

3. A SZOLGÁLAT-, BEVETÉS ÉS MENTÉSIRÁNYÍTÁSI RENDSZEREK EGYSÉGESÍTÉSNEK CÉLJAI

Ebben a pontban elsősorban infokommunikációs vetületből vizsgáljuk az egységesítés szükségességét.

Az állampolgárok ezen a területen is leginkább a modern infokommunikációs szolgáltatások által nyújtott lehetőségek maximális kihasználását igénylik, mely megfelel az érintett nemzeti és Európai Uniós irányelveknek is, ami ennek megfelelően határozta meg irányelveit. Ez tartalmazza, hogy olyan segélyhívó – fogadó-irányító szolgálatot kell kialakítani, amely képes az események hatékony kezelésére, legyen az egészségüggyel, a tűzoltási, műszaki mentési tevékenységgel, a katasztrófavédelemmel és a közszolgáltatással kapcsolatos terület. Ezen területek összehangoltság iránti igénye világszerte fokozódik, hiszen egy-egy katasztrófaesemény nem áll meg az országhatároknál (tiszai ciánszennyezés, vagy az ázsiai cunami). Ilyen helyzetekben nélkülözhetetlen az érintett szervezetek együttműködése, ahol a gyors és hatékony információáramlás, a kommunikáció életeket menthet. Egy-egy eseményen az érintett szervezetek operatív feladatai ugyan különbözőek, de minden félnek szüksége van olyan eszközökre, rendszerekre, melyek alapvető információtartalommal bírnak és képesek ezen információkat az illetékes szolgálathoz iránytani. Ezért elengedhetetlen, hogy a szervezetek kialakítsák azokat az interfészeket, amelyeken keresztül alkalmasak egymás adatainak fogadására, feldolgozására, továbbítására. Ezekről a későbbi fejezetekben bővebb információ található.

Az elmúlt években, világszerte, így az EU-ban és hazánkban is, mind a rendészet, mind a katasztrófa-elhárítás szakterületén érintett szervezetek előremutató innovációt hajtottak végre és komplex szolgálat-, bevetés és mentésirányítási, kezelési központokat, rendszereket alakítottak ki.

A 112-es segélyhívószám 1999 óta ingyenesen hívható a magyarországi vezetékes és mobil távbeszélő hálózatokból, a segélyhívásokat a Budapesti Rendőr-főkapitányság főügyelete és a megyei rendőr-főkapitányságok ügyeletei fogadják.

Az Országos Mentőszolgálat a 104 fogadására 26 központot alakított ki, a 105-ös fogadás az önkormányzati és köztestületi tűzoltóságokon történik, mindkét feladat esetében országosan több mint 180 helyen.

107-es fogadás a rendőrkapitányságokon és rendőr-főkapitányságokon történik a jelenlegi 112-es fogadási rendszerhez hasonlóan.

Az ún. „nemzeti hívószámok” (104, 105, 107) tovább élnek. Mostani elképzelés alapján nincs is tervben azok megszűntetése, és a Rendőrség által üzemeltetett 112-es segélyhívószám általi kiváltása.

A jelenlegi működés egyik legnagyobb problémája, hogy a segélyhívások fogadása és a kapcsolódó tevékenység-irányítási feladatok koordinálása egymástól eltérő módon történik, a hívásfogadásnak elvárt szolgáltatási szintje nincs, a várakoztatási idő is jelentős.

A rendőrségi informatikai rendszerek számos tekintetben támogatnak bizonyos folyamatokat, segítik a Rendőrség munkáját, azonban egységes, az erőforrások jellemzőit, státuszát, helyzetét, továbbá a komplex irányítási és koordinációs feladatokhoz szükséges egyéb információkat együttesen kezelő, a szolgálat valóban hatékony irányítását lehetővé tévő rendszer ez idáig nem került létrehozásra.

Az infokommunikációs infrastruktúra (műholdas, vezetékes, mobil távközlő rendszerek, műsorszórás), – különös tekintettel a távközlési-informatikai konvergenciára – kiemelt szerepet tölt be a kockázatok csökkentésére tett erőfeszítések rendszerében. Ennek megfelelően a katasztrófavédelmi rendszerek és készenléti szolgálatok (pl.: rendőrség, mentők, tűzoltóság, stb.) elektronizálását, korszerűsítését, - mely folyamatos állami feladat - nem elkülönülten, hanem egységesen kellene kezelni. Mivel azonban a készenléti szervezetek ragaszkodnak saját elképzeléseikhez és meg kívánják tartani az eddig kialakított rendszereiket, így jelen pillanatban nem látszik az a lehetőség, hogy egységes egészként kezelhető lenne a probléma. Ellenben bizonyos infokommunikációs területeken (pl. térinformatikai rendszerek egységesítése) most is kivitelezhető az egységesítés, ami szintén nem elhanyagolható feladat. Mégis úgy gondolom, hogy hosszútávon elengedhetetlen a katasztrófakezelésben résztvevők közös informatikai platformjának kialakítása.

4. AZ EURÓPAI UNIÓS ÉS MAGYARORSZÁGI KÖVETELMÉNYEK

Hazánk Európai Unióhoz (EU) való csatlakozásával többek között elfogadta az (Egységes Segélyhívó Rendszer) ESR kialakításának szükségességét. A magyarországi jogi szabályozás ugyan nem teljes körű, a feladat, a felelősségi körök és az irányvonalak sem egyértelműek, azonban ez nem akadályozza a készenléti szervezetek technikai fejlesztésének, működtetésének kialakítását.

5. JOGSZABÁLYI KÖRNYEZET

Az Európa Tanács még 1991-ben döntött az Egységes Európai Segélyhívó szám bevezetéséről. Az egyre gyakoribb természeti katasztrófák, az állampolgári igények, a technikai fejlődést szem előtt tartva az Európai Parlament és Tanács további irányelveket határozott meg.

Magyarország Európai Unióhoz való csatlakozásával, elfogadta ezen jogszabályi hátteret és vállalta mind a jogi, mind pedig a technikai harmonizáció végrehatását, megteremtését.

Az Európai Uniós és magyarországi jogi szabályozás tartalmazza az Egységes Európai segélyhívó rendszer bevezetésével kapcsolatos elvárások jogi hátterét, de a hazai rendelkezéseket mégsem mondhatjuk teljes körűnek, hiszen nem biztosítják a megfelelő jogi hátteret az ESR 112 kialakításához.

5.1. Az EU jogszabály követelményei

Az EU a tagállamokkal szembeni elvárásait két szinten határozza meg. Első szinten a jelenlegi, második szinten a jövőbeni szabályok, végrehatását követeli meg. Ez azért fontos szempont, mert az új rendszer kialakításánál ezt a fejlődési tendenciát tekintetbe lehet venni, mely által gazdaságosabb, hatékonyabb és egy logikailag is megfelelően bővíthető rendszer hozható létre.

5.2. Tagállami elvárások

- Segélyhívó szám: 112;
- Minden EU polgár rendelkezésére álljon 112-es segélyhívási szolgáltatása;
- A 112-es szolgáltatásnak elérhetőnek kell lennie vezetékes és mobilszolgáltatásból egyaránt;
- A segélyhívási szolgáltatásnak az év minden napján, 24 órán át folyamatosan rendelkezésre kell állnia;
- A hívó fél, és a hívás helyszínének azonosítását a távközlési szolgáltatók technikai lehetőségei figyelembevételével valósítsák meg;
- A 112-es szám használatát a távközlési szolgáltatóknak ingyenesen kell biztosítaniuk;
- A hívó fél telefonszámát el kell juttatni a hívásfogadó központba, az Eht. 145.§.(2) szerint.

5.3. Magyarországi jogszabály követelményei

- Képes legyen mind a vezetékes mind a mobil hívások fogadására;
- Az azonosító adatok (hívó fél száma, helyszíne) redundáns fogadása feldolgozása és továbbítása;
- A szolgáltatás ingyenességének biztosítása;
- Magas rendelkezésre állás pl.: biztonsági, üzembiztonsági.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A 112-es hívószámon alapuló ESR rendszer már közel 10 éve foglalkoztatja a katasztrófavédelemmel és segítségnyújtással foglalkozó szervezeteket. Mégis a konkrét megvalósítás napjainkig várat magára, amin a szakemberek nem nagyon csodálkoznak, hiszen egy olyan hatalmas, átfogó rendszer megvalósításáról van szó, amely igen komoly és időt igénylő feladat.

Jelen közlemény az egységesítés alapjait, valamint a jogi háttereket tekintette át, amely munka – reményeink szerint – alapja lehet az egységesítés témakörével foglalkozó műnek.

FELHASZNÁLT IRODALOM

[1] Magyar értelmező kéziszótár Akadémia Kiadó Bp. 1978

[2] Bakos Ferenc Idegen szavak és kifejezések szótára Akadémia kiadó Bp.1978

[3] Számítástechnikai Szótár Kossuth Kiadó, 2003

[4] Angol - Magyar Informatikai Értelmező Szótár Panem Könyvkiadó Kft. Budapest, 2004

[5] Máté József: A112-es Egységes Segélyhívó Rendszer jelene és jövője a katasztrófavédelemnél, http://www.tetraforum.hu/dokumentumok/2008/Mate.ppt (2010-03-10)

[6] Kuris Zoltán: Az egységes segélyhívó rendszer hazai megvalósításának helyzete, http://hadmernok.hu/2009_1_kuris.pdf (2010-03-10)

[7] Hanák Tibor: Katasztrófajelentési helyzete, http://www.zmne.hu/hadmernok/2008_2_hanak.pdf (2010-03-10)

[8] Új Uniós katasztrófavédelmi stratégia, http://ec.europa.eu/news/environment/090224_1_hu.htm (2010-03-12)

[9] Integrált irányító központok vészhelyzetre, http://www.siemens.hu/download/1/integralt_iranyitokozpont_veszhelyzetekre.pdf (2010-03-12)

Jelen számunk szerzői

Dorkó Zsolt r. alez.	ORFK GF ÉMGEI, osztályvezető-helyettes
Dr. Farkas Tibor fhdgy.	ZMNE Híradó Tanszék, adjunktus
Dr. Fregan Beatrix	ZMNE Nyelvi Intézet, tanár
Dr. Hóka Miklós nyá. mk. alez.	ZMNE Híradó Tanszék, egyetemi docens
Dr. Horváth Zoltán okl. mk. alez.	ZMNE Híradó Tanszék, adjunktus
Jéri Tamás bv. őrgy.	Kalocsai Fegyház és Börtön, osztályvezető
Jobbágy Szabolcs fhdgy.	ZMNE Híradó Tanszék, tanársegéd
Dr. Kassai Károly mk. ezds.	HVK HIICSF, osztályvezető
Kendernay Zsolt	KEKKH, főosztályvezető-helyettes
Dr. Kerti András mk. alez.	ZMNE Híradó Tanszék, adjunktus
Koncz Bence hallg.	ZMNE Híradó Tanszék, hallgató
Kuris Zoltán r. őrgy.	BM biztonsági vezető
Dr. Masenkó-Mavi Viktor	Budapesti Corvinus Egyetem Nemzetközi és Európa Jogi Tanszék, főiskolai tanár
Papp Zoltán őrgy.	MK AH, műveleti főtiszt
Paráda István hallg.	ZMNE BJKMK HB mérnök alapképzési szak, hallgató
Dr. Pándi Balázs	Gordon és Webster Tanácsadó NyRt., informatikai vezető
Dr. Pándi Erik r. ezds.	ZMNE Híradó Tanszék, főiskolai tanár
Pölcz Péter	CODEL Kft., ügyvezető igazgató
Dr. Rajnai Zoltán mk. ezds.	ZMNE Híradó Tanszék, egyetemi tanár
Dr. Sándor Miklós nyá. ezds.	ZMNE Híradó Tanszék, főiskolai tanár
Szabó Levente fhdgy.	MH Támogató Dandár, informatikai tiszt
Szalontai László	Budapesti Corvinus Egyetem Nemzetközi és Európa Jogi Tanszék, külső oktató
Takács Attila r. alez.	KEKKH, osztályvezető
Tóth András fhdgy.	ZMNE Híradó Tanszék, tanársegéd
Töreki Ákos fhdgy.	ZMNE Híradó Tanszék, tanársegéd

Szerzőink figyelmébe

A kiadvány lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – elsősorban: távközlés, híradás, informatika és információvédelem témakörökben – tanulmányok, szakcikkek megjelentetésére.
A cikknek tartalmaznia kell:

- egy 2-5 soros absztraktot magyar és angol nyelven;
- 2-5 magyar és angol kulcsszót;
- a cím angol nyelvű fordítását.

A cikkek beküldése e-mailen a hirado@zmne.hu címre lehetséges.
A cikkek leadási határideje: folyamatos (megjelenés évente kétszer)
A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak.
A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.
A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt írásművet - külön indoklás nélkül - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.
A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.
Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

A cikkekkel szemben támasztott formai követelmények:

Szerző(k):
Tóth András - Kovács Péter
(12 pontos ARIAL félkövér, kisbetűkkel, középre zárt)
A szerző(k) intézménye
(12 pontos ARIAL, kisbetűkkel, középre zárt)
A szerző(k) e-mail címe
(10 pontos ARIAL, kisbetűkkel, középre zárt)

CIKK CÍME

(14 pontos ARIAL, félkövér, nagybetű, középre zárt)

Absztrakt
(12 pontos Times New Roman, szimpla sorköz, dőlt, kisbetűkkel, sorkizárt)
2-5 soros magyar és angol nyelvű absztrakt. Idegen nyelvű cikk esetében is szükséges a magyar absztrakt
Kulcsszavak: 2-5 magyar és angol nyelvű kulcsszó

FEJEZETCÍM

(12 pontos ARIAL, félkövér, nagybetű, középre zárt, bekezdések előtt és után nincs beállított sorköz érték, számozás kézzel!)

A szövegtörzset Times New Roman 12 pontos betűből kell kialakítani. Sorkizárt. Sorköz szimpla. A második és minden további új bekezdés első sorát 0,5 cm-rel kell behúzni. A szövegben történő kiemelés (ha elengedhetetlenül szükséges) dőlt betűkkel, nincs félkövér kiemelés a szövegben. Lábjegyzet: Times New Roman 10 pontos betű, szimpla sorköz, sorkizárt, sem előtte, sem utána nincs beállított térköz! Ne használjunk stílusokat!
Ábrákat, képeket, valamint a táblázatokat középre rendezve, a képaláírást vagy a táblázat nevét a kép/ábra illetve a táblázat alá középre Times New Roman 12 pontos betűből kell elkészíteni. Minden képnél, ábránál és táblázatnál meg kell adni a forrást is!
Nincs oldalszámozás. Élőfej és élőláb területe üres.

Alfejezetcím

(12 pontos ARIAL, félkövér, kisbetű, középre zárt, bekezdések előtt és után nincs beállított sorköz érték! Az alfejezetek számozása kézzel történik.)

A szövegtörzset Times New Roman 12 pontos betűből kell kialakítani. Sorkizárt. Sorköz szimpla. A második és minden további új bekezdés első sorát 0,5 cm-rel kell behúzni. A szövegben történő kiemelés (ha elengedhetetlenül szükséges) dőlt betűkkel, nincs félkövér kiemelés a szövegben. Lábjegyzet: Times New Roman 10 pontos betű, szimpla sorköz, sorkizárt, sem előtte, sem utána nincs beállított térköz! Ne használjunk stílusokat!
Ábrákat, képeket, valamint a táblázatokat középre rendezve, a képaláírást vagy a táblázat nevét a kép/ábra illetve a táblázat alá középre Times New Roman 12 pontos betűből kell elkészíteni. Minden képnél, ábránál és táblázatnál meg kell adni a forrást is!
Nincs oldalszámozás. Élőfej és élőláb területe üres.
Irodalmi hivatkozás (Times New Roman, 12 pontos betűk, balra rendezve, bekezdés után 6 pont). A szerzők a cikk témájától függetlenül szabadon választhatnak a számozott, vagy a névszerinti módszer között.

Számozott hivatkozások:
A hivatkozásokat a szövegben való előfordulásuk sorrendjében számozzuk, a szövegben a hivatkozási számot szögletes zárójelben tüntetjük fel, pl. [1]. Az irodalomjegyzékben a számozott hivatkozások bibliográfiai elemeit az alábbi minták szerint adjuk meg:
FOLYÓIRATCIKKRE
[1] P. Smith, E. McGregor: Effect Based Operations in Afghanistan. Military Journal, 62 (2007) 482-490.
KÖNYVRE
[2] R. Cook, P. R. Hammer: *Military Inventions in the World War II*. United Press, 1990.
KÖNYV VAGY MONOGRÁFIA FEJEZETÉRE
[3] K. Wells: The reasons of the terrorist attacks. In: K. Wells, R. Pupil (Eds), *2006 Islam in the 21th Century*. United Press, 2006.
Névszerinti hivatkozások:
Az irodalomjegyzékben a hivatkozásokat számozás nélkül, abc-rendben soroljuk fel. A szövegbeli hivatkozás a szerző nevével és a megjelenés évszámával történik, pl. "Kovács (1990) szerint" vagy "egy korábbi tanulmány (Kovács, 1990) szerint". Ha ugyanattól a szerzőtől és ugyanabból az évből több munkára hivatkozunk, azokat lássuk el megkülönböztető jelzéssel (pl. a,b,c). Az irodalomjegyzékben a névszerinti hivatkozások bibliográfiai elemeit az alábbi minták szerint adjuk meg:
FOLYÓIRATCIKKRE
Smith, P., McGregor, E. (2007): Effect Based Operations in Afghanistan. Military Journal, 62:482-490.
KÖNYVRE
Cook,R., Hammer, P. R. (1990): *Military Inventions in the World War II*. United Press.
KÖNYV VAGY MONOGRÁFIA FEJEZETÉRE
Wells, K. (2006): The reasons of the terrorist attacks. In: In: K. Wells, R. Pupil (Eds), *2006 Islam in the 21th Century*. United Press.

Kézirat publikációs céllal történő benyújtása

HÍRVILLÁM SIGNÁLBANDA

Az alábbi cikket a *Hírvillám* című folyóiratban kívánom megjelentetni:

A kézirat címe: .....

.....

.....

A szerző*

neve: .....

munkahelye: .....

levelezési címe: .....

telefonszáma: .....

FAX száma: .....

e-mail címe: .....

Aláírásommal igazolom, hogy a publikációs céllal benyújtott kézirat eredeti, saját munkám, amely még nem jelent meg máshol, és eddig nem is nyújtottam be ilyen céllal máshová.

A kézirat minősített anyagot, vagy minősített információt nem tartalmaz.

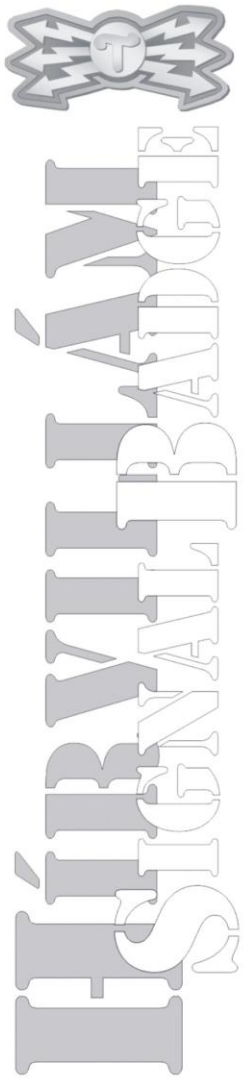
A kéziratban a szerzői jogoknak megfelelő módon vannak jelezve a hivatkozások, idézések, azok jelen írás szerzői jogainak átruházását nem érinti.

Kelt: .....

.....
a szerző aláírása

* több szerző esetén minden személynek külön kitöltött „Kézirat beküldési űrlap”-ot kell mellékelni a kézirathoz

Copyright átruházási nyilatkozat



Az alább megjelölt cikk copyright jogait az alább megnevezett szerző vagy szerzői kollektíva átruházza a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszékére, ha és amikor a cikket közlésre elfogadják. A copyright jogok magukban foglalják a cikk sokszorosításának és terjesztésének jogait beleértve a fotografikus, elektronikus vagy bármely más hasonló technikával történő másolás, ill. a fordítás jogát is.

A nyilatkozatot aláíró szerző aláírásával tanúsítja, hogy a cikk eredeti és hogy birtokában van az átruházandó jogoknak, valamint hogy felelősséget vállal az összes társalkotó nevében is a copyright jogok átruházásának jogosságát illetően.

A szerzők a publikált cikket saját honlapjukon hozzáférhetővé tehetik az Interneten, feltéve, hogy feltüntetik a megjelenés pontos bibliográfiai adatait, az elérhetőség címét (URL), és a copyright tulajdonosaként a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék nevét.

A cikk címe: .....

.....

.....

Szerző(k)

neve:	aláírása:
.....	.....
.....	.....
.....	.....
.....	.....

Kelt: .....

Felelős kiadó: Prof. Dr. Rajnai Zoltán mk. ezredes
Megjelent a ZMNE Híradó Tanszék gondozásában, 10 példányban, illetve elektronikusan:

www.puskashirbaje.hu

HU ISSN 2061-9499

***

ZMNE BJKMK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-358 mellék)
hirado@zmne.hu