

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM



Kommunikáció – 2006

Communications – 2006



Zrínyi Miklós Nemzetvédelmi Egyetem
Budapest, 2006. október 25.

A tudományos kiadványt szerkesztette:

Dr. Rajnai Zoltán mk. alezredes

Lektorálták:

Dr. habil. Sándor Miklós ezredes
Szöllősi Sándor okl. mk. őrnagy
Kerti András mk. őrnagy
Kis Lajos mk. százados

Idegen nyelvi lektor:

Fregan Beatrix

Felelős kiadó: Prof. Dr. Szabó Miklós akadémikus, a Zrínyi Miklós Nemzetvédelmi Egyetem rektora
Megjelent a Zrínyi Miklós Nemzetvédelmi Egyetem gondozásában

Készült a Zrínyi Miklós Nemzetvédelmi Egyetem nyomdájában, 200 példányban
Felelős vezető: Kardos István

(A publikációk tartalmáért és minőségéért a szervezők nem vállalnak felelősséget.)

ISBN: 978-963-7060-18-2

TARTALOMJEGYZÉK

Dr. habil.Sándor Miklós nyá. ezredes	
A híradótisztek egyetemi képzésének megteremtése	12
Vörös Béla nyá. ezredes	
Amit a híradásról tudunk — 1956	18
András Magyar - Gyula Mikó - Rudolf Seller	
Aspects of Direction Estimation in Mobile Communication Systems	28
Balázs Pándi:	
Core Communications Network – an international overview	37
Szabó András	
Kihívások a Magyar Honvédség elektronikus adatkezelő rendszerének hitelesítése terén	42
Bánfi Tibor	
Digitális rendszerek alkalmazása a kínai katasztrófa elhárításban	53
Máté József pv. alezredes	
Monitoring és Lakossági Riasztó Rendszer megvalósítása	66
Dr. Ványa László:	
Út a szoftverrádiók és szoftver rádiózavaró állomások felé	76
Dr. Vass Sándor alezredes:	
Az infokommunikációs berendezések elektronikai védelmének néhány aktuális kérdése	84
Vörös Béla nyá. ezredes, okl. villamosmérnök:	
Egyetemünk 1956-ban	101
Tessedik Tamás:	
Az információ biztonság stratégiai menedzsmentje	111
Dr. Haig Zsolt mk. alezredes	
Információs támadás és hatásai	119
Kassai Károly	
Az elektronikus információvédelmi rendszabályok megalapozásának fontosabb kérdései	131
Sándor Magyar – Dr. Miklós Sándor:	
The advantages and possibilities of the IP based telecommunication in peace support missions	144
Balázs Pándi	
Reformation of the military core networks	149
Maros Dóra	
Veszélyhelyzeti távközlés	154

Pál Tamás	
Lépésenkyszer és lehetőség a közigazgatásban	168
Balázs Pándi	
Problems of the Core Communications Network	179
Szöllősi Sándor okl. mk. őrgy.:	
A magyar katonai híradás perspektívái	184
Erik PÁNDI:	
Closed-purpose systems contra governmental centre of electronic public services	192
Erik PÁNDI:	
Competitive civil service – queries of development	198
Péter Kovács - András Magyar - Rudolf Seller	
Radar Cross Section Reduction Using White Noise Controlled RCS	202
Dr. Sipos Mihály:	
Jelenkori elektronikai iparunk főbb ökonómiai és geográfiai változási tendenciái	209
Attila Takács	
New challenges in the area of European electronic government	223
Németh András okl. mk. főhadnagy:	
A katasztrófavédelmi kommunikáció alternatív megoldásai	227
Schuller József Attila:	
Mobil munkavégzési megoldások a Kapschtól	256
Gábor Egri	
Information technology in policing in the european union the schengen information system	261
Révész Gyula mérnök alezredes	
A kor kihívásai a kiképzők szemével	273
Erik PÁNDI:	
Outsourcing of communication services in the field of public administration	280
Attila Takács	
The status of the electronic civil service nowadays	284
Kis Lajos mk. százados:	
A vezetési pont hírközpontok modernizálása, avagy optikai eszközök a vezetési ponton	289
Kerti András mk. őrnagy:	
A vezetés és a hírendszerek kapcsolata	293
Rajnai József (SIEMENS):	
Hogyan tovább? Útkeresés a Magyar Honvédség hírendszereiben	302

Fregan Beatrix :	
L'avancée des perspectives européennes	312
Fazekas Béla (T-Systems):	
Közigazgatási szolgáltatások a Magyar Telekom NYrt-től	317
Patrice Erulin (Alcatel):	
The Network Transformation	326
Bozsó Zoltán rendőr ezredes:	
Rendőri intézkedések rendje a sportlétesítményben és azon kívül	330
Megyeri Sándor (VT-Rendszertechnika Kft.)	
A Magyar Honvédség követelményei alapján kifejlesztett	
20'-as zárt felépítmény család	333
Dr Medveczki Zoltán orvos őrnagy:	
Életmentő beavatkozások fül- orr- gége sérülések esetén	339
Szvétek Ferenc (FERCOM):	
Small Dimetra IP Compact system	349
Jean-Louis DEBEURET (THALES):	
Tactical Internet et Postes de Commandement	354
Dr. Zoltan Rajnai – Laszló Trembeczky	
SATCOM et interoperabilité	360
Breitner Gábor	
Műholdas távközlési eszközök és szolgáltatások	362
Vígh Levente	
Információvédelmi szempontok és a WiMAX	
alkalmazási lehetőségei	366
Dr. Dárdai Árpád	
Biztonsági és Diszpécser Rádiótelefon rendszer	378

A nemzetközi szakmai tudományos konferencia
kommunikációs partnere:

Magyar Telekom ZRt

... **T** ... **Systems** ...

A tudományos konferencia támogatói:



ALCATEL Hungary Kft.

SIEMENS ZRt.

THALES COMMUNICATIONS

KONGSBERG HUNGÁRIA Kft.



Kapsch Kft.



Fercom Kommunikációs Kft.



VT- Rendszertechnika Kft.

C-Vision
Vizuálkommunikációs Kft.



Alcatel Hungary Kft.
1116 Budapest, Kondorfa u. 10.
Tel.: (+36-1) 209-9500
www.alcatel.hu

A NEMZETKÖZI KONFERENCIA HÁTTÉR INFORMÁCIÓI

A konferencia fővédnöke:

Mikita János mk. altábornagy, MH Honvédszerkezet vezérkar főnök helyettes

A konferencia védnökei:

Prof. Dr. Szabó Miklós vezérőrnagy, akadémikus, ZMNE rektor

Horváth Ferenc dandártábornok, Híradó és Informatikai Parancsnokság parancsnok

A konferencia kommunikációs partnere:

Magyar Telekom ZRt.

A konferencia támogatói:

ALCATEL Hungary Kft.

SIEMENS ZRt.

Thales Communications

Kongsberg Hungária Kft.

Kapsch Kft.

Videoton Rendszertechnikai Kft

FERCOM Kommunikációs Kft.

C-Vision Vizuálkommunikációs Kft.

A konferencia rendezői:

Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék

Hírközlési és Informatikai Tudományos Egyesület ZMNE Egyetemi Csoport

A szervező bizottság elnöke:

Dr. Rajnai Zoltán mk. alezredes

A szervező bizottság titkára:

Dr. habil. Sándor Miklós ezredes

A szervező bizottság tagjai:

Szöllősi Sándor okl. mk. őrnagy

Kerti András mk. őrnagy

Kis Lajos mk. százados

Előszó

A Tisztelt Olvasó az évenként rendezett „Kommunikáció - Communications” tudományos konferencia kiadványát tartja a kezében.

A tudományos-technikai fejlődés egyre gyorsabb változásának eredményeként ma már az infokommunikációs technológia 8-12 havonta megújul. A változások irányát a napi biztonság és katonapolitikai-gazdasági döntések módosítják. Ezen belül kiemelt szerep jut a katonai, kormányzati kommunikációs megoldásoknak, a változó kommunikációs technikáknak és technológiáknak, a hozzájuk kapcsolódó szervezeti és képzési problémák megoldásának.

A könyvben közreadott és vizsgált témák időszerűségét jelzi, hogy a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék, a Honvéd Vezérkar, a Hadtudományi és Katonai Műszaki Doktori Iskolák valamint a Hírközlési és Informatikai Tudományos Egyesület ZMNE egyetemi csoportja által rendezett „Kommunikáció 2006” nemzetközi szakmai tudományos konferencián elhangzott előadások egy részének szerkesztett változatát olvashatjuk.

A tudományos cikkek szerzői többségében kutató intézetek, egyetemek, kormányzati és polgári távközlési szervezetek tudományos munkatársai, oktatói, doktoranduszai.

A tudományos konferencia célja volt a katonai kommunikáció EU, NATO és hazai hadműveleti vezetés rendszerében elfoglalt helyének, szerepének értelmezése és képet adni a katonai képzés és felkészítés aktuális kérdéseiről és a velük összefüggésben levő feszítő problémákról a haderő korszerűsítéssel folyamatosan változó környezetben. Erősíteni kívánta a nemzetközi és nemzeti katonai, kormányzati és polgári szakértők szervezett tapasztalatcseréjét és rendszeres kapcsolattartását.

A konvergencia megjelenési formáit a konferencián kiállított és a résztvevők intézményeinél már hozzáférhető kommunikációs rendszerek és hálózatok példáin keresztül mutatta be.

A szervező bizottság nem titkolt szándéka, hogy az előadásokon elhangzottak minél szélesebb körben ismertté váljanak, ezért a könyv mellett – *korlátozott példányszámban* – az elhangzott előadások prezentációit elektronikus változatát is közreadja.

*Dr. Rajnai Zoltán alezredes
tanszékvezető, egyetemi docens*

Dr. habil.Sándor Miklós nyá. ezredes

A híradótisztek egyetemi képzésének megteremtése

Az 1990-es évek elején nem csak a politikai, gazdasági és társadalmi változások foglalkoztatták intenzíven a ZMKA tanári állományát - *köztük a Híradó tanszéket* -, hanem a felsőoktatás átalakításával, az intézmények, hallgatók és oktatók jogállásával, jogaival, kötelességeivel összefüggő új törvények megjelenése is.

Ezek az új törvények, jogszabályok új nézőpontból és új szemlélettel kezelték a felsőoktatást mind intézményi, mind a hallgatói autonómia vonatkozásában. Új irányt szabtak a tudományos képzésnek és továbbképzésnek is. Új alá- és fölérendeltségi viszonyok alakultak ki, amelyek természetesen érdekeket sértettek, amelyek esetenként jelentősen befolyásolták az intézmények és a minisztériális szervek kapcsolatát. A legjellemzőbb példa erre a Nemzetvédelmi Egyetem jogállása, alárendeltsége. A törvény a Honvédelmi Miniszter felügyelete alá helyezte az egyetemet, ezzel a Vezérkari Főnök dominanciája megszűnt.

Ilyen nagy ívű, sodró időszakban érkeztünk el az 1993-as évhez, amikor is az Országgyűlés elfogadta az 1993.évi LXXX törvényt a felsőoktatásról. A törvény hatálya a Magyar Köztársaság területén működő összes felsőoktatási intézményre, így a főiskolai képzést folytató Bolyai János Katonai Műszaki, a Kossuth Lajos Katonai, és a Repülőtiszti Főiskolára, hanem az egyetemi szintű képzést folytató Zrínyi Miklós Katonai Akadémiára is egyetemlegesen vonatkozott. A törvény rendelkezése alapján a Zrínyi Miklós Katonai Akadémia neve Zrínyi Miklós Nemzetvédelmi Egyetemre változott. Az addig önálló státusú katonai főiskolák az egyetem főiskolai karai lettek, majd a későbbiekben beintegrálódtak az egyetem kari szervezetébe. Így a ZMNE három karral, - *a hadtudományi, a vezetés- és szervezéstudományi egyetemi és a Bolyai János Katonai Műszaki Főiskolai Karral* - indította el, illetve folytatta tovább a képzést.

A ZMKA Híradó tanszéke - *a képzési profil és az oktatói állomány megőrzésének nem titkolt szándékával* - Katonai Kommunikációs Rendszer-szervező Tanszékre változtatta a nevét a csoportfőnök támogató jóváhagyásával. Az eddigi szakmai alá- és fölérendeltség helyébe korrekt, mély szakmai elkötelezettségen alapuló, esetenként komoly vitáktól sem mentes kapcsolat lépett. Az idő előre haladtával, közben 1996-ban az Országgyűlés elfogadta az 1996. évi XLV. Törvényt, mely a katonai és rendvédelmi felsőoktatási intézmények vezetőinek, oktatóinak és hallgatóinak jogállásáról rendelkezett. Természetesen az átalakításoknak, átalakításoknak esetenként fájdalmas személyi konzekvenciái is voltak. Tény, hogy a ZMKA Híradó tanszékének 1990-ben 25 fő volt az oktatói és a közalkalmazotti állománya. Ez a létszám a ZMNE

KKRSZT megalakulásával 1995-ben 18 főre, 1998-ban 11 főre, majd 2005-ben 6 (!) főre csökkent. Természetesen ezekbe a létszámcsoökkentési hullámokban mindig az éppen aktuális haderő csökkentési, haderő átalakítási, haderő fejlesztési koncepciók érvényre juttatása fejtette ki áldásos hatását. Természetesen közben a kötelező óraszámok állandóan nőttek, az oktatói állomány-nal szembeni követelmények is a permanens emelkedés pályájára álltak.

A tanszéken 1991-ben egyetemi doktori címet szerzett 1 fő, 1992-ben 1 fő, 1995-ben 1 fő, 1996-ban 1 fő és 1997-ben 1 fő. A doktori képzés átalakulásával 1997-ben 2 fő kezdte meg PhD tanulmányait, melyet 2001-ben és 2002-ben sikeresen meg is védtek. 2001-ben egy fő teljesítette a habilitációs követelményeket, és habilitált doktorrá avatták. 2005-re a tanszéken 3 fő rendelkezett a követelményeknek megfelelő tudományos fokozattal, míg 2 fő doktori képzésben vett részt. A 2005-ös évben hosszú várakozás után összevo-násra került a ZMNE KKRSZT és a BJKMF Híradó tanszéke egy új szerve-zetben a Bolyai János Katonai Műszaki Karban Híradó tanszék néven.

De térjünk vissza 1993-ra.

A felsőoktatási törvény megjelenése egy jókora, mondhatni hatalmas követ dobott a felsőoktatás megjegecesedett állóvizébe. Rendelkezései hatalmas hullámokat kavartak. Különböző szervezetek szűntek meg, alakultak át és ki, változtak meg, mire kialakult a ZMNE, annak is a Vezetés- és szervezéstudományi kara. A szervezeti keretek kialakítása, kialakulása után egy többlépcsős, többfunkciós munka vette kezdetét. Meg kellett /volna!/ találni azt az optimális keretet, amelyben a kar tanszékei a képzési profiljuknak megfelelő keretekben, szakonként folytathatják oktatási, képzési tevékenységüket. Érvek és érdekek csaptak össze, majd következett a hatalmi szó. Ennek megfelelően alakult ki, jött létre a Haditechnikai menedzser szak négy szakiránnyal.

Katonai kommunikációs rendszerszervező szakirány
Védelmi informatikai rendszerszervező szakirány
Katonai elektronikai rendszerszervező szakirány és a
Katonai üzemeltető és rendszerfejlesztő szakirány.

E felsorolásból is látható, hogy a szakon három szakirány rokon, ille-tőleg rokonítható, mert az alap mindhárom esteében az elektronika, míg a ne-gyedik egy haditechnikai - *durva megfogalmazás szerint* - páncélos és gépjár-műves, fegyveres szakirány. A szak felelőse természetesen a Haditechnikai tanszék gépészmérnöki végzettségű vezetője lett, bár a másik három tanszéken még két tanszékvezető is egyetemi tanári beosztást töltött be. Mindezek termé-szetesen nem befolyásolták alapvetően a képzési koncepció kialakítását, vi-szont a tanórák elosztásánál a hatalmi szó érvényesült a szakmai elvárásokkal,

követelményekkel szemben. A szakok és a szakirányok kialakítása után 1994-ben megkezdődhetett a tantervek kialakítása, összeállítása.

Ahhoz, hogy az egyetem ne csak a nevében legyen az és azt meg is tarthassa sikeres akkreditáció esetén, ötéves alapképzéssel és kiegészítő /nappali és levelező/ alapképzéssel kellett rendelkeznie. Mivel a szak neve adott volt, meg kellett határozni a képzési célt, azon belül is az általános értelmiségi, illetve a katonai-szakmai képzés célját, a szakirányok specifikus célkitűzéseit, a képzés időtényezőit. El kellett készíteni a mintatanterveket, meg kellett határozni a kritérium követelményeket, a szakmai /csapat/ gyakorlatok időtartamát, a záróvizsgák követelményeit, stb. Ebben a kis dolgozatban a szak okmányaival nem, illetve csak a szükséges mértékben kívánok foglalkozni.

A jelentős kompromisszumok hatására sikerült a szak képzésének általános célkitűzését megfogalmazni. A Haditechnikai menedzser szak képzésének általános célja: a Magyar Honvédség, illetve más fegyveres testületek és az ezekhez kapcsolódó polgári szféra részére olyan szakemberek képzése, akik a megszerzett társadalomtudományi, általános értelmiségi, hadtudományi, katonai műszaki, vezetés-és szervezéstudományi elméleti és gyakorlati ismereteik, jártasságaik és készségeik alapján képesek békében és háborúban a működési területeiknek megfelelő katonai műszaki-technikai, szervezési és vezetési feladatok alkotó megoldására. A katonai kommunikációs rendszerszervező szakirány képzési célkitűzése a következőképp alakult: olyan kommunikációs rendszerszervező tisztek, honvédségi közalkalmazottak, köztisztviselők képzése, akik az elsajátított korszerű társadalomtudományi, természettudományi, hadtudományi és módszertani ismereteik felhasználásával, egy idegen nyelv kellő ismerete /felsőfok C!/ képesek a fegyveres testületek kommunikációs rendszereinek tervezésére, szervezésére, létesítésére és irányítására. Az egész életpályát megalapozó korszerű általános és katonai alapképzés kialakítása, melynek birtokában, feladatkörében alkalmassá válik eszméi értékek alkotó közvetítésére, létrehozására. Az oklevélben megjelölt szakképzettség:

Okleveles haditechnikai menedzser, a betétlapon: Katonai kommunikációs rendszerszervező.

Az egyetemi alapképzés:

Képzési idő: 5 év /10 félév/, legalább 3900 tanóra

A képzés főbb tanulmányi területei és arányai:

- általános művelő, értelmiség képző tudományterületek: 26%
- általános katonai felkészítést biztosító tananyag: 6%
- vezetési ismeretek és szakalapozó tantárgyak: 35 %
- szakmai tananyag: 33 %

A képzés során matematikából, közgazdaságtanból, hálózatok és rendszerekből, valamint parancsnokok és törzsek felkészítése, a híradócsapatok kiképzése című tárgyakból kellett szigorlatot tenniük a hallgatóknak. A záróvizsga komplex számonkérés volt. A záróvizsgán az és csak az vehetett részt, aki először a vizsgabizottság előtt sikeresen megvédte szakdolgozatát. A záróvizsga szóbeli része négy tantárgyon alapult: vezetés és szervezéselmélet, rendszerben tartás elmélete, valamint két szakmai tárgy, a katonai kommunikációs rendszerek tervezése és a katonai kommunikációs rendszerek szervezése.

A tantárgystruktúra kialakításánál alapul vettük egyfelől a BJKMF Híradó tanszékén a villamosmérnök képzésben oktatott tantárgyakat annak ellenére, hogy nem villamosmérnök képzést folytattunk, másfelől a tanszéki kollektíva állásfoglalását, véleményét, amelyeket egyeztetettük a szakmai irányítást végző csoportfőnökséggel. A politikai, katonapolitikai helyzet változásai-ból adódó változások hatására úgy döntöttünk, hogy nem kerülhet ki az egyetemről, nem kaphat oklevelet az a kommunikációs rendszerszervező /híradó/ tiszt, aki alapjaiban ne ismerné a Magyar Köztársaság kommunikációs infrastruktúráját, a hálózatmenedzsment és a hálózat felügyelet problémakörét. Nem kis büszkeséggel említem meg, hogy a mi tanszékünk, a mi szakirányunk volt az egyetlen, ahol ötéves tiszti alapképzés folyt, s ezzel alapjaiban járultunk hozzá az egyetemi akkreditáció sikeréhez. Sajnos nem rajtunk múlt, hogy egyetemi alapképzést – *a haderőfejlesztési változások, változatok hatására* - csak két alkalommal, két tancsoportban indíthattunk. Az 1999-2004-es képzési időszakra beiskolázásra került 18 fő, melyből egy fő közlekedési balesetben elhunyt, egy fő lemorzsolódott. Egy fő kiváló tanulmányi eredményei ellenére nem kapott diplomát, mert nem tudta teljesíteni a felsőfokú nyelvi követelményeket. A 2000-2005-ös kiképzési időszak végén 9 fő kapott diplomát.

A tancsoportok felkészültségére, felkészítettségére csak két adatot szeretnék bemutatni:

KMKA-1 osztály államvizsga átlaga:4,40

KMKA-2 osztály államvizsga átlaga:4,41

Csak zárójelben jegyzem meg, mielőtt valaki elfogultsággal vádolna, hogy a vizsgabizottság öt tagjából kettő külsős, szakmailag magasan kvalifikált szakember volt. Az egyetemné válás, az egyetemi képzés továbbra is lehetőséget biztosított a főiskolai diplomával rendelkezők részére egyetemi diplomát szerezni kiegészítő egyetemi alapképzés keretében. A felvételi követelményeket teljesítő hallgatonál vizsgálni kellett a parancsnoki hozzájárulás és az előírt szigorlatok meglétét, azokat, amelyek az ötéves egyetemi alapképzés első 2 évében kerültek oktatásra. A hiányzó szigorlatok esetén intézkedni kellett azok pótlására. Meg kellett vizsgálni azt is, hogy a főiskolai lecke-köny-

vekben rögzített, már lehallgatott tantárgyak tartalma ekvivalens-e az egyetemi képzésben oktatott tantárgyakéval, vagyis elfogadható-e a hallgató vizsgája az adott tantárgyból, felmenthető-e a tantárgy lehallgatása alól, vagy kötelezni kell-e a tantárgy felvételére. A kiegészítő egyetemi alapképzést két formában - *nappali és levelező* - indítottunk. A nappali képzésben résztvevők négy, a levelező képzésben részesülők hat szemeszterben - *szemeszterenként két kéthetes összevonással* - teljesítették tanulmányi követelményeiket. Az első kiegészítő alapképzésű tancsoport 1997.09.01-jén 8 fővel kezdte meg tanulmányait KMKK-1 tancsoport néven. Egyenesen lenyűgöző volt azt érzékelni, hogy ezek a hallgatók nem a diplomáért, hanem a megszerezhető tudásért jelentkeztek a képzésre. Az első év tanulmányi átlaga 4,35, a második évé 4,41 volt. A tanszék oktatói és közalkalmazotti állománya a tanév kezdetére jelentősen, 11 főre csökkent a soros átszervezések eredményeként. 1998.09.01-jén indítottuk el az első levelező kiegészítő egyetemi alapképzésű tancsoport képzését 10 fővel.

Jelentős erőfeszítéseket tettünk a tananyag folyamatos korszerűsítésére, mely néha nem ment súrlódásmentesen, mert jelentős ellenállásba ütköztünk a szak képviselői, vezetése részéről. Jelentős áttörést a 2000-es esztendő hozott, amikor is jelentős tananyag korrekciót, tananyagfejlesztést sikerült végrehajtanunk. Nagyon sok erőfeszítésünkbe került az állandó koncepció változásból következő hadseregfejlesztést tananyaggal lefedni, csak a csapatokkal kialakított jó kapcsolataink felhasználásával sikerült ezeket a problémákat is sikeresen megoldani. A kreditrendszerű képzés beindítása, a nappali kiegészítő egyetemi alapképzés elsorvadása - *a tisztek féltették beosztásukat, azért nem jelentkeztek nappali képzésre* - a levelező képzés idejének csökkentése újból nagy erőfeszítésre készítette a tanszék állományát, mely további véraldozatokkal öt főre csökkent. A HM döntése következtében az eddigi három éves levelező képzésünket két évre kellett csökkenteni. A hallgatók a két tanulmányi év alatt 384 kontaktórában kapják meg mindazokat az ismereteket, amelyek számukra az egyetemi diploma megszerzéséhez elengedhetetlenül szükségesek. Természetesen ez permanens otthoni tanulás nélkül nem teljesíthető.

Általános ismeretek: 42 tanóra, 420 munkaóra /otthoni/, 14 kredit, 11,67%

Általános katonai, rendvédelmi ismeretek: 46 tanóra, 420 munkaóra, 14 kredit, 11,67%

Szakmai ismertek: 296 tanóra, 2760 munkaóra, 92 kredit, 76,66%

Ezen elvek alapján készül a jelenleg végzős KMKL-4B osztály és az elsőéves KMKL-5B osztály. Az egyetemmé válás óta a tanszék kiveszi a részét az egyetem doktori iskoláiban folyó doktorandusz képzésből is. Jelenleg a

Hadtudományi- és a Katonai Műszaki Doktori Iskolában egy önálló és két egyesített tudományszakon folytatunk témavezetői és oktatói tevékenységet. Napjainkban 12 fő témavezetését végezzük.

A tanszéki infrastruktúra folyamatosan változott. Elődeink nagyszerű munkája eredményeként jelentős infrastruktúra állt rendelkezésre. Az egyetemi képzés beindításakor 7 szakkabinettel és 5 általános felhasználású kabinettel rendelkezünk. A kor kihívásainak megfelelő kabinetek kialakításához, felszereléséhez a különböző kormányzati szervek pályázatain mintegy 65 millió Ft-ot nyertünk és építettük be. Sajnos a szakmai szervektől, akik részére a képzést végezzük egy fillér támogatás sem érkezett. A tanszék tudományos felkészültségéről, tudományos szervezőmunkájáról, nemzetközi elismertségéről az évenként megrendezendő nemzetközi szakmai tudományos konferenciákon ad számot, melyeken jelentős szellemi potenciál jelenik meg. A konferenciák nem titkolt kimondott és kimondatlan céljával tüztük ki, hogy vizsgáljuk a távközlés helyzetét a Magyar Honvédség, a kormányzati szervek, valamint a közcélú és külön célú távközlő hálózatokhoz kapcsolódó szervezetekben. Áttekinteni a kommunikációval kapcsolatos trendeket és kihívásokat a XXI. században. Bemutatni az élenjáró akadémiai és felsőfokú oktatásban az infokommunikáció terén folyó tudományos kutatások eredményeit. Elemezni a katonai kommunikáció/híradás/ szerepét, a konvergencia megjelenési formáit a híradás szervezésében. A képzés és a felkészítés szakma specifikus jellemzőinek vizsgálata a változó környezetben. A Magyar Honvédség híradásának biztosításában résztvevő távközlő vállalatok szolgáltatásainak megismerése. Erősíteni a szervezett tapasztalatcserét és rendszeres kapcsolattartást a hazai és a nemzetközi partnereinkkel. Mára az évenként megrendezendő Tudomány Ünnepe rendezvények kiemelt eseményévé nőtte ki magát és növeli a tanszék presztízsét.

A COMMIT francia –magyar híradó gyakorlások megteremtésével lehetőséget sikerült biztosítanunk hallgatóink és oktatóink részére a szakmai felkészülés és látókör kiszélesítésére.

És eljött a 2005-ös esztendő. De ez már egy más történet.

Vörös Béla nyá. ezredes

Amit a híradásról tudunk — 1956

A mindenkori kormány védelmi tervet készített azoknak az objektumoknak a fegyveres védelmére, melyek a biztonságos polgári működést, az ország államvédelmi, rendőri és katonai védelmét irányítani tudják. Erre saját belső titkosított automata telefonközpont, akkori szóhasználattal „K” vonal szolgált. Ezen kívül minden fegyveres szervezetnek saját híradása volt. A polgári híradást a fővárosban automata telefonközpontok biztosították. Az országban tartózkodó szovjet csapatoknak saját híradásuk volt, emellett a magyar hírhálózatot is használták. Közös gyakorlatokon, ha azt két vagy több nemzet hajtotta végre, mindenkinek saját híradása is volt. Az előljáró, irányító Varsói Szerződés parancsnoksággal a híradást a szovjetek biztosították. A polgári híradást biztosító személyek állása mindig bizalmi állás volt. Katonás fegyelem uralkodott, a személyeknek rendfokozatuk volt, a fegyelmi szabályzat is hasonlított a honvédségben használatos követelményekhez, és a büntetés is komoly volt. A fenti okok miatt, a híradást biztosító intézmények védelmét minden társadalmi rendszerben katonailag is biztosították. A legfontosabbakat békében is éjjel-nappal belügyi őrség védte.

A tárgyalt időszakban, témánkkal kapcsolatban a terv szerint az alábbi megerősítéseket kapták volna:

Védelmi erők elosztása körzetenként és bázisonként: (részlet)

- I. körzet: Körzetparancsnok: ZMKA parancsnoka: Márton András ezredes
Rádió stúdió 1/3 órs Belügyminisztérium
Zrínyi Miklós katonai akadémia:
Közlekedés és postaügyi minisztérium, Főposta
„Erzsébet” távbeszélőközpont
„Teréz” távbeszélőközpont
- II. körzet: Körzetparancsnok: a Petőfi Politikai Tiszti Iskola parancsnoka:
Lakihegyi adó BM 2/3 órség 39 fővel
Operatív rádióadó BM Soroksár 4 fő rendőr
Távbeszélőközpont Kispest : Petőfi Sándor politikai tiszti iskola
Távbeszélőközpont Pesterzsébet -,-
- III. körzet: Körzetparancsnok: Ságvári Endre Hadtáp Tiszti Iskola parancsnoka
Kossuth Tüzér Tiszti Iskola:
Távbeszélő központ Újpest 7 fő
Kőbányai távbeszélő központ 7 fő
Zuglói távbeszélőközpont 7 fő
Petőfi Politikai Tiszti Iskola:
Posta rádióvevő központ 7 fő
Marcheyi elosztó 7 fő

IV. körzet: Körzetparancsnok: Sztálin Katonai Politikai Akadémia parancsnok: Pesti Endre ezredes.

Operatív rádióállomás-I	1 szakasz BM karhatalom
Operatív rádióállomás-II	ua
Operatív rádióállomás-III	ua.

Akadémia:

Rádió (Baba u.14.):	7 fő
Zugliget távbeszélő központ:	1 lövészraj (7 fő)
Óbudai távbeszélő központ	1 raj
Krisztina távbeszélő központ	1 raj
Szabadsághegyi TB központ	1 raj

V. körzet: Körzetparancsnok: Zalka Máté Híradó Tiszti Iskola parancsnoka: Susa István alezredes

Rendőrség:

Rádióadó	Dobogóhegy	4 fő
Rádióadó	Diósd	
Főposta		

Vasvári Pál Tiszti Iskola:

Diósd-i rövidhullámú rádióállomás	1 raj
Lágymányosi távbeszélő központ	1 raj
Budafoki távbeszélő központ	1 raj

A védelmi terv nem volt „naprakész”, mivel éppen ebben az időben fontos változások zajlottak, így ezt a tervet végrehajtani nem lehetett!

Néhány változás:

- A budapesti Híradó Tiszti Iskola kiköltözött Szentendrére,
- A Vasvári Tiszti Iskola maradéka elköltözött Szolnokra,
- A Ságvári Hadtáp Tiszti Iskola maradéka a Zrínyi akadémiába olvadt,
- A Petőfi Tiszti Iskola helyet változtatott

A fenti okok miatt az eredeti terv szerint nem lehetett dolgozni, ezért a feladatok és a végrehajtók összekeveredtek. Számos nem katonai feladatot át kellett venni a feloszlott államvédelmi hatóságtól.

Végül a káoszt fokozta, hogy amikor eldőlt a hatalom kérdése, a legtöbb alakulat visszament helyőrségébe. A további őrzést a megalakult nemzetőrség vette át, illetve az alakulatok forradalom mellé állt állománya.

Telefonközpontok védelme

A Zrínyi Miklós Katonai Akadémia egy kisebb csoportot indított útba a *Krisztina* telefonközpont védelmére. A távbeszélő központok ezekben az években fontos katonai objektumok voltak. Az együttműködést a Posta Katonai Szolgálat biztosította, amely az adott postán kapott elhelyezést. Ennek a védelme is fontos katonai feladat volt. A fő feladatot a Híradó tanszék beosztottjai kapták, mint akik szakmailag is ismerték az objektumot. A telefonközpontot határőrökkel is megerősítették a budapesti határőr-híradókat kiképző központból. A védőknek a többszöri fegyveres támadás ellenére sikerült a központot október 30-ig megtartani. Ezután alkudozás kezdődött, és a központot további őrzésre, november 2-án átadták a kijelölt nemzetőr csoportnak, és bevonultak az akadémiára. A nemzetközi összeköttetéseket lebonyolító *József* telefonközpont is fontos védelmi góc volt, melyet a 102. rádiófelderítő ezred egy csoportja védett, Gyuricza Imre alezredes parancsnoksága alatt, kiegészítve az akadémistákkal. A központ épületét négy szovjet harckocsi is védte. Ezt a központot is támadták a fegyveresek, például rálöttek a szovjet katonákra a közeli templom tornyából. A járőr elfogta a lövöldözőt, aki egy fiatal gyerek volt. Amikor a szovjet harckocsik parancsot kaptak, hogy ki kell vonulni Budapestről, akkor a nagy kapkodásban a központban felejtettek egy szovjet főhadnagyot, és a Romániából idevezényelt 33. motorizált alakulattól itt ragadt 3 szovjet "harcost", akik a Corvin-kőnél elvesztették csapatukat és ide hozták őket. Innen vitte ki őket Tökölre Fomin szovjet alezredes, aki akkor a Különleges Hadtestnél volt tolmács.

Itt kell megjegyeznem, hogy a hallgatók és a növendékek részére a "választóvíz" a Szabad Nép cikke, a HAJNALODIK volt, amely az eddigi eseményeket népfelkelésnek nevezte, így a kirendelt intézmények és alakulatok akik fegyveresen védték a "néphatalmat" nem tartoznak a forradalmárok közé. Hogy a további összetűzéseket elkerüljék, a parancsnokok feladták a védendő objektumokat, és visszatértek a laktanyákba. A Szabad Nép vezércikkéből - *ami az akkori egyetlen pártnak a Magyar Dolgozók Pártjának a hivatalos lapja volt* - továbbá az is kiderült, hogy akik eddig a hatalmat védték, azok lettek a néppellenesek, akik ellen felléptek, azok lettek a nép akaratát végrehajtó forradalmárok. A második szakaszban a hadsereg az új kormányának határozatának megfelelően tagja lett a megalakult Nemzetőrségnek. Egyes alakulatai az új honvédelmi miniszter - Janza Károly altábornagy - parancsai szerint cselekedtek. Ennek a parancsnak a lényege az volt, hogy a hatalmat a fegyveres erők és a felkelőkből alakult forradalmi egységek közösen gyakorolják. Ennek érdekében azokat is fel kellett fegyverezni, akiknél eddig nem voltak fegyverek.

A szocialista rendszer kommunikációs eszközeinek védelmében

A többi iskolával együtt a tatai lövész és harcokcsizó tiszti iskola is megkapta a karhatalmi riadó parancsot október 23-án késő éjjel. Összeállították a menetoszlopot, amelynek első lépcsőjét az iskolán tanuló államvédelmi és határőr növendékek alkották. Azt a parancsot kapták, hogy vonuljanak a rádióhoz, az ott lévő egységek megerősítésére. Budapest bejáratához közeledve, már várta az oszlopot Hegyi vezérőrnagy és a Budai Nagy Antal légvédelmi tüzér laktanyába irányította őket. Az oszlop előtt haladó elővéd túljutott már a Bécsi úton, és beért a rádióhoz. Az iskola parancsnoka Szilágyi Dezső alezredes volt. Az iskola állományát több csoportban vetették be 24-én.

Zakócs János őrnagy parancsnoksága alatt 6 tehergépkocsival, mintegy 150 fő lövész növendék indult útba a rádióhoz, hogy visszafoglalja azt. A lövész rajokat géppuskások egészítették ki. Mire a csoport beért a rádióba - kb. *délelőtt 10 órakor* - a felkelők már elfoglalták a rádió épületét. A zászlóalj állománya 8 tiszt, 150 lövész szakirányú növendék. Fegyverük karabély volt, amit 3 db Gorjunov géppuska egészített ki. A tiszteknél pisztoly volt, 14 db lőszerezrel.

A rádiót más egységek segítségével sikerült visszafoglalni, és október 30-ig megtartani. Fegyveres harcra nem került sor. A rádiót 23-án este elfoglaló csoportok az ostrom következtében az épületekben és a szobákban rengeteg kárt okoztak, berendezéseket törtek össze, iratokat szórtak szét, a magnetofonszalagokat letekerték stb.

A csoport más idevezényelt alakulatokkal őrizte a rádió épületeit. Október 28-án itt is megalakították a Katonai Tanácsot, és teljesítették mindazokat a parancsokat, melyeket a honvédelmi miniszter a napok folyamán kiadott. (új megszólítás, rendfokozati jelzések átalakítása, sapkacsere, stb.)

Az iskola hősi halottjának Patai Mihály hadnagynak a története is a rádióhoz kapcsolódik. Az ott lévő növendékek részére gépkocsin élelmiszert szállított. Visszafelé jövet a Rákóczi úton erős tüzet kaptak, melyben Patai mellett még két halott és három sebesült is volt. A gépkocsi megsemmisült. Érdekessége az esetnek, hogy Patai hadnagy halálát mindössze "szolgálati balesetnek" minősítették, és hosszú hónapok múltán kapta meg családja azokat a juttatásokat, melyek abban az időben kijártak egy hősi halottnak.

A lakihegyi adótoronynál

A másik csoportot (páncélos hallgatók) a Lakihegyen lévő rádióadóhoz vezényelték. A rádióadót az ott lévő államvédelmi őrség védte: 2 tiszt, egy hivatásos őrmester, és 50 fő sorozott államvédelmi sorkatona. Az adót már 23-án este körül vette egy kb. 40 fős civil felfegyverzett csoport. A védők megakadályozták az adótorony elfoglalását, közülük több foglyot ejtettek, akiket 27-ig az épületben őriztek, majd elszállították őket a központi börtönbe.

Ennek a csoportnak a megerősítésére a tatai tiszti iskola páncélos zászlóalját jelölték ki. Létszámuk 6 tiszt, 90 növendék. Parancsnok: Szabó Sándor főhadnagy, helyettese Zámbo Sándor főhadnagy volt.

25-én a védelem kiegészült 3 db 85 mm-es légvédelmi löveggel, 1 fő tiszttel és 40 sorkatonával.

26-án ismét erősítés érkezett. 3 db harckocsi, 1 fő tiszt és 12 fő sorkatona jött az esztergomi harckocsi alakulattól.

27-én délután 60 fő érkezett Pécsről. Ekkor az államvédelmi csoport elvult.

Az adóállomást komolyabb támadás az időszak alatt nem érte. Szórványos lövöldözések előfordultak. Ettől két harckocsizó katona sebesült meg. A tiszti iskolának ezt a zászlóalját 30-án az objektumból kivonták. Az adóállomás további őrzését sorkatonák vették át. A forradalom alatt a Kossuth rádió végig sugárzott. Egy ízben a rádiónál dolgozók szakszerű segítségével Csepel határában átvágták a stúdiót és az adótornyot összekötő kábelt. Ezt a hibát sikerült fegyveres fedezet mellett elhárítani, miközben a kis csoportot a felkelők igyekeztek feladatukról lebeszélni. Azt nem tudták, hogy a Duna alatt is létezik egy kábel, amely tovább biztosította kerülő úton a kapcsolatot a stúdiót helyettesítő ideiglenes - *parlamentben kialakított* - stúdióval.

Műsorszolgáltatás

A forradalom idején a műsorszolgáltatás a parlamentben kialakított stúdióból történt. Mivel itt a technikai biztosítás szűkös volt – *mindössze néhány hangszóró és mikrofon* – az adás és a szolgáltatás ennek megfelelő volt. A Parlamentet a parlament őrsége, a kirendelt erősítés, és a szovjet katonai erők védték, az adás lehetősége biztosított volt.

Zrínyi Miklós Katonai Akadémia

A forradalom legszembetűnőbb híradó feladatait a Corvin-közi csoportnál hajtotta végre a ZMKA híradó tanszéke. Az ide kiveényelt Haász János: *Tettem valamit a hazámért* című könyvéből tudhatjuk meg, melyet az egyetem adott ki. A híradással kapcsolatos feladatokat Koncz Mihály tanszékvezető és helyettese Kolozsvári Sándor irányították. A Corvin-közi azt a feladatot kapták, hogy a több helyen lévő csoportok között teremtsenek összeköttetést. Ezt városi vezetékes vonalon és rádió is megoldották. A rádiós rendszerbe bevonták a híradó ezredet és a repülőteret. Rövid vezetékes híradást létesítettek a Práter utcai iskola és a kisebb csoportok között. A megvalósító állomány a „katonaságnál” a híradóknál szolgált. Az esőlemez távbeszélő központot egy orvosgyógyászati leány kezelte. A rádióállomások R-40 és R-50 típusúak voltak. A nagyteljesítményű rádióállomás az Üllői út sarkán lévő házban települt. Az oroszok támadása után külfölddel is tartott összeköttetést

RÓKA adó néven. Az adó parancsnoka Orosz Mihály főhadnagy, aki akkor hallgató volt az akadémián. Haász olyan parancsot is kapott, hogy szervezze meg a PARTIZÁN moziban a híradók továbbképzését. Erre azonban már nem került sor.

A Nemzetőrség ellenállása

Király a rendelkezésére álló nemzetőr egységek között igyekezett az összeköttetést megteremteni. A Kakukk-hegyen lévő rádiókat kívánta üzembe helyezni. Talált is ehhez egy műszerészt. Ennek ellenére a rádiókat nem sikerült működésbe hozni. A Széchenyi-hegyen települt zavaró rádióállomást azonban elfoglalta. Azon keresztül közleményt adott le, melyben ellenállásra buzdított. Megbízta Tancsin Miklóst, hogy a hegyekben lévő nemzetőr csoportok között szervezze meg a híradást. Vezető állomás feladatait a közeli határőrlaktanyából szerzett R-40 típusú rádióállomással kívánták megoldani, míg tagállomásoknak hordozható rádiókat terveztek. Az R-40 gépkocsiba épített rádióállomás, a Nagyszénási turistaházban települt. Néhány nemzetőr csoporttal sikerült a kapcsolatot megteremteni. Összeköttetésben állnak:

- Solymár nemzetőrség
- Piliscsaba nemzetőrség
- Budai kenyérmalom
- Bp. Keleti-Károly u. csoport

A váltott közleményekben többek között a nemzetőr főparancsnok figyelmezteti a csoportokat, hogy tartózkodjanak az egyéni akcióktól. Oláh Vilmos arra kapott parancsot, hogy menjen vissza a Széchenyi-hegyre, és hozzon el még egy rádiót. Ezt a parancsot már nem tudta végrehajtani, mert a Labanc úton a határőrök elfogták őket. Kihallgatásukkor a technikára vonatkozólag az alábbi vallomást tették:

- a vezetési pont a Nagykovácsi kastélyban van,
- a Nagykopasz-hegyen van 1 légvédelmi üteg, 8 löveggel,
- a Zsíros-hegyen 1 légvédelmi üteg szintén 8 löveggel,
- a Kakukk-hegyen 1 légvédelmi üteg

Szállító járművek: 1 db 3 tonnás szállító gépkocsi, 1 db Fiat tehergépkocsi, 1 db raj gépkocsi, 2 db személygépkocsi, 1 db páncélozott gépjármű, 4 db fogatolt jármű.

Híradó eszköz: 6 db kisorádió, 1 db nagyteljesítményű rádióállomás.
(Szovjet források szerint 5 gépkocsit, és 15 rádióberendezést foglaltak le.)

Dunapentele: október 31-én a Nemzeti Bizottság letartóztatta a régi katonai vezetőket. Kivitték az **R/40 rádióállomást**, majd Szabad Dunapentele névvel sugárzott főleg nyugatra. November 5-e után tovább működött mint *Rákóczi adó*.

Székesfehérvári: Vadásztölténygyár udvarán **telepített R/40 rádióállomás** összeköttetést tartott a hadtest laktanyájában telepített rádióállomással. Amikor a szovjetek tűz alá vették a gyári rádióállomást, Nagy Rudolf tizedest, aki fel tartott kézzel jött ki a rádiós kocsiból, több lövéssel lelőtték. Miután bementek a kocsi belsejébe, a bent lévő két katonát is tűz alá vették. Jáki István és Szabó István honvédek megsebesültek. Miután Jáki megmozdult, további sorozatot lőttek rá, meghalt. Szabó István, aki nem mozdult, később – *mintegy hat óra múlva*- elsősegélyben részesítették majd kórházba szállították.

A budapesti híradó ezred szerepe az 1956-os forradalom napjaiban

Komoly fegyveres katonai alakulat 1956. októberben nem volt Budapesten. Éppen folyt az átszervezés. Rendelkezésre állt az azonnali bevetésre a Budapesten állomásozó híradó ezred. Ezt és még más kisebb, nem harcra felkészített alakulatot vetettek be 1956. október 23-án este. A Budaörsi úton lévő híradó ezredet mozgósították a Magyar Rádiónál összegyűlt tömeg feloszlására. A feladatot maga az ezred parancsnoka Móricz Ferenc alezredes vezette. Az ezredet 20 óra 20 perckor riadóztatták. A *kivezényelt* részleg azt a feladatot kapta, hogy a Bródy Sándor utcában összegyűlt tömeget oszlassa szét. Az ezred kivezényelt részlege mintegy 210 fővel 21,10-kor érkeztek a rádióhoz vezető Bródy Sándor utca elejéhez. Lőszert nem kaptak, fegyverük náluk volt. A gépkocsioszlop a Bródy Sándor utca bejáratánál megállt. A katonák leszálltak. A parancsnok a gépkocsik őrzésére 2-2 főt hagyott vissza. A tervezett oszlatás nem sikerült, mert a tömeg észre vette, hogy a katonáknak nincs lőszerük. Megtámadták magát a parancsnokot is, akit gépkocsivezetője védett meg. A hátrahagyott katonák közül az összetűzésben életét veszítette Borgula András tizedes. A sikertelen feladat végrehajtás után a kivezényelt katonákat 22 órakor visszavitték a laktanyába. A kirendelést és a visszavonulást a híradó főnökség ügyeletese végezte. A laktanyát is támadás érte. A polgári tüntetők fegyvert követeltek, miután ezt nem kapták meg, elmentek. Másnap, 24-én az ezred a forgalom ellenőrzését végezte, főként a gépkocsin utazó forradalmárok közlekedését akadályozta. Az összetűzések következtében több forradalmárt letartóztattak. A laktanyának az őrzését megszigorították, az őrseget megerősítették. Az ezred parancsot kapott más híradó objektumok védelmére is. Így Mé-

száros Béla őrnagy csapata kapta feladatul a Híradó Szertár védelmét, a mellette lévő ruházati raktárral. Felföldi Lajos főhadnagy vezetésével járőrözést folytatott az ezred. A IX. kerületben igazoltattak, eldobált fegyvereket szedtek össze.

Október 25-én egy csoport a Déli Összekötő vasúti híd megerősítésére kapott parancsot. A 30 híradó katonával ellátott feladatot segítette Kapitány Antal főhadnagy. A híd őrzésében a másik hídállást szintén védték Nagy János és Nyári György főhadnagyk parancsnoksága alatt. Amikor Nagy főhadnagy telefonálni ment, a forradalmárok elkapták és kísérőivel együtt lefegyverezték. Ezután indult fegyveres támadás a híd védői ellen. A tűzharcban három honvéd is megsebesült. Elkezdődött a katonák meggyőzése az átállásra. Hídfő másik oldaláról megindult a segítség. Végül a hidat egy harckocsiból álló egység mentette meg. A híradó ezred katonái helyet álltak, leváltásuk után bevonultak a laktanyába.

26-án az ezred járőrözött. Eldobált fegyvereket szedték össze. P I főhadnagy vezetésével 100 fő a Szabadság-hídat védelmezte sikeresen. 27-én 200 fővel a Móricz Zsigmond körteret és környékét ellenőrizte. Hajnalig járőröztek.

28-án az ezred parancsot kapott a Pártközpontot védő Híradó Tiszti Iskola növendékeinek a leváltására. Ezt a feladatot Mészáros Béla őrnagy kapta. Az ezred még továbbra is ellátott feladatokat, például október 29-én 50 fővel védte a DISZ központot, és még számos feladatot kapott. Az sem véletlen, hogy a híradó laktanyában kapott szállást, a Budai Parancsnokság Itt érte őket november 4-én a hajnali szovjet támadás.

A híradó tiszti iskola elköltözött Szentendrére. Ennek ellenére a harckészültségi tervekben még mint Budapesten lévő alakulat szerepelt. Övé volt az 5.körzet.

5. VÉDELMI KÖRZET

XI. és XXII. kerület

Körzetparancsnok: Zalka Máté Híradó Tiszti Iskola parancsnoka: Susa István alez.

Rendelkezésre álló erők :

Híradó Tiszti Iskola 114 ti. 20 tts. 25 honvéd 271 növ., össz.: 430 fő

Vasvári Tiszti Iskola 175 ti. 69 tts. 563 honvéd 79 növ., össz. 886 fő

Ker.osztályok 18 ti. 237 tts. 14 egyéb össz.: 289 fő

Mindösszesen: 1605 fő

fegyverzet: 315 pu / karabély / 224 gpi. 60 gs. 8 gpu.

Védendő objektumok :

Rendőrség :	kerületi tanácsok	4-4 fővel
	kerületi pártbizottságok	
	rádió Dobogó-hegy	
	rádió Diósd	
	főposta	
	Szovjet emlékmű Gellért-hegy	
BM őrség:	Budakeszi lőszerraktár	2/2 őrs. + 13 fő
	Diósd lőszerraktár	2/4 őrs. + 10 fő

Zalka Híradó Tiszti Iskola: Budaörsi út 49-63 18 fős őrség

Közp.ruharaktár	1 raj
Híradó szertár	1 raj
Kelenföld pu.	2 szakasz
Kábelgyár Hadiüzem	1-1 szakasz
Beloianisz gyár	
Gamma	
Bp. Sodronykötélgyár	
Hidrogén és oxigén gyár	
Országos gabonátároló	

Vasvári tiszti iskola: Budaörs Kőérberki u

Repülőtér	45 fő
robbanóanyag raktár	29 fő
Háros, mű.ag.raktár	26 fő
Bányagyutacsgyár	1 szakasz
Kinizsi elosztó /Háros/	1 raj
Lágymányosi távbeszélő központ	
Budafoki TB.közp.	
Diósd rövidhullámú rádióállomás	
Keményfémipari vállalat	
Prés és kovácsológyár Hü.	
Kismotor és gépgyár Hü	
Fogaskerékgyár	

HM őrzászlóalj:	MNVK 2. Csf-ség - 8 fő
OLLEP + Szikla	16 fő
OLLEP pk-ság.	8 fő
Helyőrség Kom.Hivatal	13 fő
Pol.főcsf-ség.lőszerraktára	4 fő

egyéb objektumok: 20.OLLEP hír.e.	18 fő őrség
Vasúti hidak	
Bp-i főo. 4-4 fővel	
Tartalék: Híradó ti.iskola:	2 század
Vasvári ti.iskola	2 század
állománya iskolánként:	164 fő
	82 pu.
	50 gpi
	18 gsz.
	4 gpu
	6 t.gk.

Ezt a tervet sem tartották be, távbeszélőn riadóztatták a növendékek 2. és 3. évfolyamát. A híradókat a pártközpont védelmére, a műszakiakat a belügyminisztérium védelmére rendelték ki, október 23-án este. Mindkettő Budapesten volt. A mozgósított erő, gépkocsin tette meg az utat. Minkét objektumban volt védelmi erő, főként államvédelem. A pártközpontot határőrség is védte. Rövid időn belül *-még aznap éjjel felé* - szovjet csapatok is érkeztek az objektumok védelmére. Az összehozott védelmi erő megakadályozta, hogy a két objektumot a támadók elfoglalják. A híradó tiszti iskola híradási feladatokat nem látott el.

A növendékek leváltásuk után bevonultak az iskolára.

1. Introduction

The importance of the capacity growth of data transfer channels has increased mainly due to higher data transfer demands on the side of end users. In mobile radio systems several methods exist to extend the capacity of the radio system, one of them is the Space Division Multiple Access technique. This technique requires smart antennas to divide the even space into several separated spatial radio channels; the main functions of these antennas are: EM spatial spectrum estimation to determine the number and position of radio sources, Digital Beam Forming (DBF) to form the mentioned separated radio channels. In this paper EM spatial spectrum estimation is dealt with. The aim of EM spatial spectrum estimation is to obtain information on the position and radiation strength of radiating EM sources. This is achieved by sampling the EM field in space, considering Shannon's law of sampling in space analogue with sampling in the time domain. Samples are taken with antenna elements, being attached to the electronic channel that samples the signal appearing at the antenna output and converts it to digital data, which is sent to the central computing unit (PC). Spatial spectrum estimation is considered narrow-band in the frequency domain in this case, theoretically single frequency CW signals are considered in the calculations. The scheme of such a channel system can be seen in Fig.1.

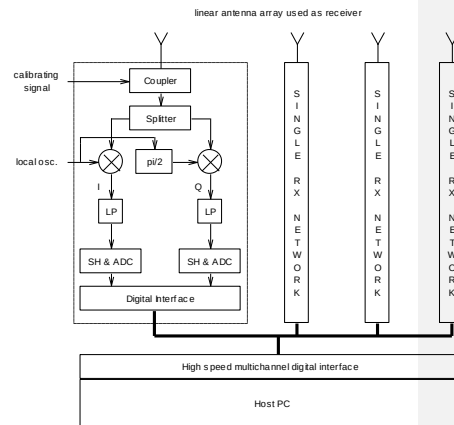


Figure 1.: The system blocks

Channels must be synchronized in phase and the static amplitude and phase differences of the channels must be compensated (the antenna system must be calibrated).

In our research spherical and rectangular grid antenna element arrangements were investigated, focusing on rectangular grid arrangements.

2. Spatial spectrum estimation theory

The direction of narrow-band radio sources present in the measured area is estimated by antenna arrays that measure the amplitudes and phases of the EM wave generated voltage, generated at the antenna elements, using the well known Fourier-relation between the far-field field strength distribution of the EM environment and the electric or magnetic field strength distribution on the antenna aperture. We suppose isotropic radiator antenna elements.

First we specify an n -element antenna structure, then we measure the $n \times n$ estimated correlation matrix $\hat{R}$ of the structure. If the complex representation of the k -th electric field vector on the aperture of the antenna array is:

$$\mathbf{z}_k = [r_{1k}e^{j\varphi_{1k}} \dots r_{ik}e^{j\varphi_{ik}} \dots r_{nk}e^{j\varphi_{nk}}], \quad (1)$$

where r_{ik} and φ_{ik} are the actual amplitudes and phases of the incoming EM wave at the place of antenna element i ,

then the estimated correlation matrix is

$$R_k = [r_{ik}e^{j\varphi_{ik}} r_{jk}e^{-j\varphi_{jk}}]_{i,j} \text{ and } \hat{R} = \frac{1}{M} \sum_{k=1}^M \mathbf{z}_k * \mathbf{z}_k^H = \frac{1}{M} \sum_{k=1}^M R_k, \quad (2)-(3)$$

where M is the number of samples taken in the time domain.

The real correlation matrix is then $R = E\{\hat{R}\}$.(4)

The more samples are taken the less variance will the estimated correlation matrix have.

The most obvious spatial spectrum estimation method is the so called Fourier- (or Bartlett-) method, where the field strength distribution on the antenna array aperture is being correlated with a supposed plane wave field strength distribution, that is, Fourier-transformation is done on the measured correlation matrix. The spatial spectrum is obtained by applying different supposed plane waves with different angles of incidence in the Fourier-transformation.

This method yields relative high peak sidelobe levels (PSL) in the estimated spatial spectrum and the resolution of the measurement will also be relatively low. To achieve higher resolution larger antenna arrays would have to be implemented and to achieve lower PSL different amplitude transmissions of RF channels would have to be achieved. Since this requires extensive investments and the practical size of such antenna arrays is also limited, another

solution would be preferable. The resolution and the PSL together form the performance of the spatial spectrum estimation method.

To achieve better performance so called adaptive spectral estimator methods were developed, some of these are: MSINR (Capon) method, MEM, MUSIC. The antenna array aperture field strength distribution of the supposed incident plane EM wave is represented with the scanning vector S .

The Bartlett-method:

The estimated spatial power spectrum for 1 dimension ($\mathcal{G}$):

$$P(\mathcal{G}) = S^T(\mathcal{G}) R S^*(\mathcal{G}), \text{ where } R \text{ is the } \mathbf{nxn} \text{ correlation} \quad (5)$$

matrix of the structure. In practical cases when R is estimated by M pieces of samples in time $\hat{R}$, the estimated correlation matrix is used.

The MSINR (Capon) method:

The estimated spatial power spectrum for 1 dimension ($\mathcal{G}$):

$$P(\mathcal{G}) = \frac{1}{S^T(\mathcal{G}) R^{-1} S^*(\mathcal{G})}, \text{ where } R \text{ is the } \mathbf{nxn} \text{ correlation} \quad (6)$$

matrix of the structure. In practical cases when R is estimated by M pieces of samples in time $\hat{R}$, the estimated correlation matrix is used.

Comparison of methods

The following figures show the performance of spatial spectrum estimation methods. 2 non-correlated sources of the same strength are simulated separated by 20° in azimuth (-10° and $+10^\circ$), both being at the 0° elevation angle. The change of resolution capabilities of methods can be observed in Fig. 2., first with the Bartlett-method then with Capon and MUSIC. The figure shows the results of the spatial EM spectrum estimation methods, that is, the estimated angular power distribution of incident EM waves at the antenna array aperture, in 2 dimensions in this case (Theta: elevation angle, Phi: azimuth angle).

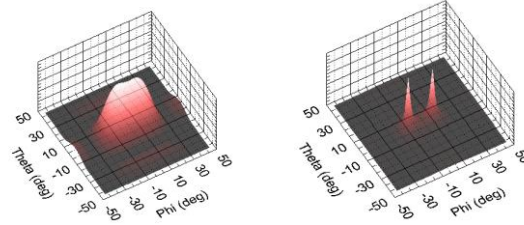
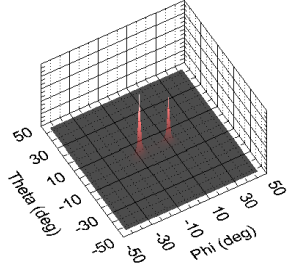


Figure 2.: DOA estimator algorithms: Bartlett, Capon, MUSIC



Simulation parameters: SNR: 10dB, sample number: 100.

3. Array calibration

In order to achieve correct sampling of the EM environment with the antenna elements and the electronics they are attached to, forming the RF channels of the antenna array, the transmission differences of these RF channels must be compensated. This can be achieved with inbuilt expensive hardware solutions, however, software compensation is also possible. This can be achieved with the inputting of known calibration signals into the system as shown in Fig. 1. Since the calibration signal is known the RF channel transmission can be calculated and during measurements the measured values can be compensated by these transmissions in the computer.

Channel transmissions can have large variance and they also vary with time, henceforth, antenna array calibration is a necessity in most cases. In order to achieve low level calibration to ensure continuous measurements spread spectrum calibration signals can be used.

4. Antenna structures, MRA - rare element structures

The resolution of an antenna array, utilized for DBF, both in transmission and reception directions or for spatial spectrum estimation, is mainly influenced by the antenna array structure. The wider the antenna array is the higher will the resolution be, that is, the main lobe of the antenna array will be narrower. In the case of spatial EM spectrum estimation adaptive methods help achieve narrower main lobes resulting in higher resolution, however, also in the case of adaptive methods the main lobe width is strongly influenced by the size of the antenna array. According to the needs of the system an achievable resolution must be defined and to this resolution the proper antenna structure must be selected.

In case of need for higher resolution and less need for low sidelobe levels MRA (Minimum Redundancy Arrangement) structures can be used. This is based on the redundancy of the full $n \times n$ estimated correlation matrix $\hat{R}$ of the

equidistant structure. That is, if some elements are omitted from the full equidistant grid all correlation values of the EM environment might still be present in the estimated correlation matrix. This is shown for a linear case below.

The correlation matrix in a general case is the following for a linear structure:

$$R = \begin{bmatrix} R_0 & R_1 & R_2 & R_3 & \cdots \\ R_{-1} & R_0 & R_1 & R_2 & \cdots \\ R_{-2} & R_{-1} & R_0 & R_1 & \cdots \\ R_{-3} & R_{-2} & R_{-1} & R_0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

R_i matrix element means the correlation between antenna elements at i distance from each other. Redundancy means in this case that matrix R contains an element more than one time. This is demonstrated for a 4 element structure in Fig. 3. below.

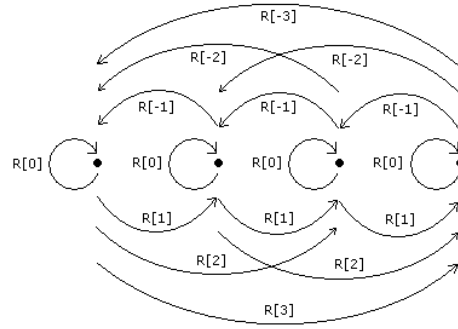


Figure 3.

If we consider a 7 element full linear array we can omit some elements to reduce the redundancy of matrix R while keeping at least one of all matrix elements.

This is demonstrated in Fig. 4. below.

In this case the correlation matrix will be redundancy free, apart from the

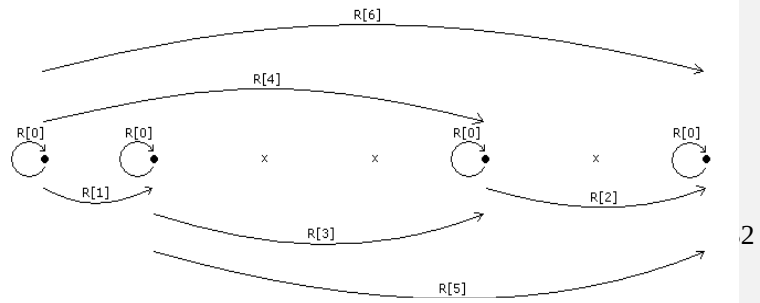


Figure 4.

multiple non-avoidable autocorrelation elements R_0 .

An example for this is shown below for a 4 by 4 full and rare element antenna array.

The 4 by 4 frame of the rare element structure is shown in Fig. 5. (switches up show antenna elements present and down show antenna elements absent), simulation results comparing the full array and the rare element array are shown in Fig. 6. Fig. 6/a., for the full array and Fig. 6/b. for the rare element array. Simulations were done with the Bartlett- and with the Capon-method.

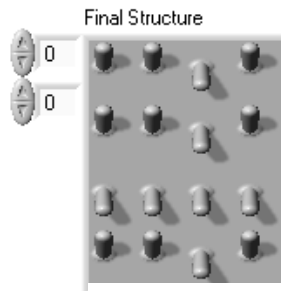


Figure 5.

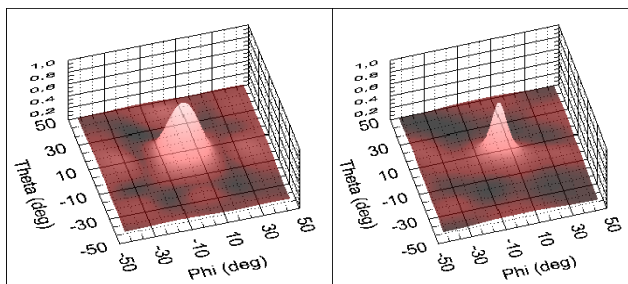


Figure 6/a

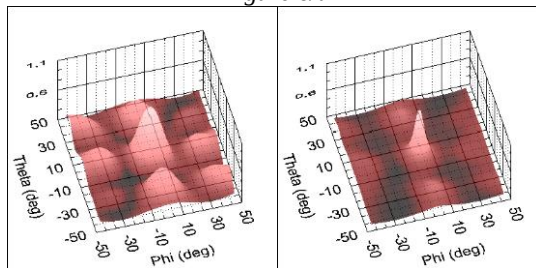


Figure 6/b

Although with the conventional Bartlett-method the rise of the sidelobe level is significant, with the Capon- and few other adaptive spectral estimator methods this rise is less significant, providing good resolution and peak sidelobe level (good performance) solutions for systems with spatial spectrum estimation function.

5. Correlated sources

In practical cases especially in urban locations due to the presence of reflecting surfaces (due to metal construction parts mainly) signals arrive at the receiver antenna array on multiple paths. This yields the singularity of the measured correlation matrix of the antenna array. If adaptive spectral estimator methods are to be used, hence most of them are based on the inversion of the correlation matrix, the singularity of the correlation matrix is to be cancelled.

Several correlation canceller methods are known, two of them are discussed now.

Redundancy averaging: the method is based on the artificial shaping of the correlation matrix by averaging the diagonals in it, and all elements on a diagonal are substituted by the appropriate average value. This method does not reduce the degree of freedom in direction estimation, however, it causes detectable stationary measurement errors.

Spatial averaging: this method divides the antenna array into multiple, overlapping sub-arrays with equal element-number. Due to the less sensor elements in one sub-array the maximal number of signal sources distinguishable by the system is decreased, we lose degrees of freedom, whereas, this method does not cause stationary measurement errors. In Figure 7/a. and 7/b. two sub-array structures can be seen.

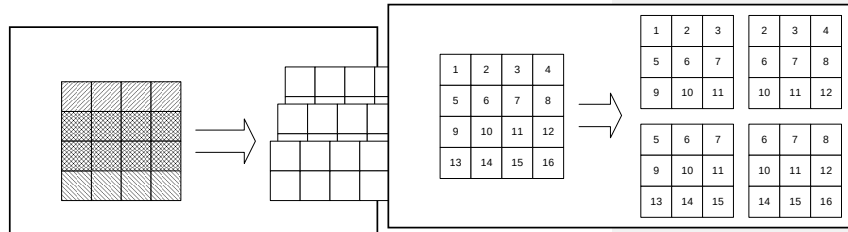


Figure 7/a.: Sub-array arrangement Figure 7/b.: Sub-array arrangement

Generally, it can be said that the number of separable sources in one dimension, azimuth or elevation, depends on the number antenna elements in one row. The structure in Figure 7/a. can handle more targets and gives better

resolution in the azimuth plane and worse in the elevation plane. Figure 7/b. shows a uniformly good arrangement for both planes. The resultant correlation matrix, from which we calculate the final results, in this case, is the average of the correlation matrices of the sub-arrays.

The correlation matrix of the k-th sub-array, where $\mathbf{x}_k$ is the vector of the signals of the sub-array elements:

$$\mathbf{R}_k = E[\mathbf{x}_k \mathbf{x}_k^H]. \quad (8)$$

The estimation of matrix $\mathbf{R}_k$, calculated from M pieces of samples:

$$\hat{\mathbf{R}}_k = \frac{1}{M} \sum_{m=1}^M \mathbf{x}_{km} \mathbf{x}_{km}^*. \quad (9)$$

The resultant estimated correlation matrix is calculated below, where K is the number of sub-arrays:

$$\hat{\mathbf{R}} = \frac{1}{K} \sum_{k=1}^K w_k \hat{\mathbf{R}}_k. \quad (10)$$

The simplest method is when the w_k coefficients have the same value, practically unit value. It is possible to combine those sub-matrices adaptively or with a static rule.

A measurement example to demonstrate the capabilities of spatial averaging is shown below in Fig. 8. Capon-method is used, the source was located at 0° elevation and azimuth.

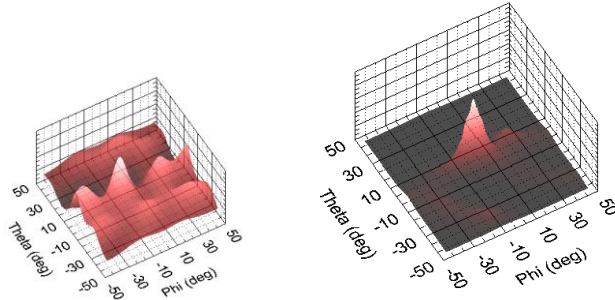


Figure 8.: Capon-method without spatial averaging and with spatial averaging

Conclusion

Research has been conducted on the utilization of smart antennas in mobile systems. Research results of spatial EM spectrum estimation for mobile systems were presented: antenna array structure selection considerations, the importance and possible ways of antenna array calibration, the problem of the negative effect on spatial EM spectrum estimation of multipath propagation and solutions and the aspects of algorithm selection have been discussed. Our researches were supported by simulations and measurements with a C-band antenna array, capable of narrowband sampling and the utilization of any desired spatial EM spectrum estimator algorithm.

We would like to conduct research in the UMTS frequency band, based on our experience in the C-band: the effects of EM wave propagation properties on smart antenna usage, the construction of a UMTS frequency band spatial sampler antenna array with the same main features as our C-band system to justify our theoretical research results and simulations.

Acknowledgements

This work was supported by the Mobile Innovation Center, Hungary.

References

- [1] John Litva, Titus Kwok-Yeung Lo: *Digital beamforming in wireless communications*, Artech House Publishers, 1996.
- [2] Darel A. Linebarger, Don H. Johnson: *The Effect of Spatial Averaging on Spatial Correlation Matrices in the Presence of Coherent Signals*, IEEE Transactions on Acoustics, Speech and Signal Processing. Vol. 38. No. 5. May, 1990.
- [3] A. Manikas: *Evaluation of Superresolution Array-Techniques as applied to Coherent Sources*, International Journal of Electronics: 22nd September 1997.
- [4] Mikó, Gy.; Magyar, A.; Seller, R.: *Adaptive Radio Direction Finding Measurement Results and the Aspects of Measurements, Investigated with a Re-configurable, 16-channel Radio Direction Finder Antenna Array*, 7th COST 284 Workshop, Chexbres, Switzerland, March 2-4., 2005.
- [5] Gyula Mikó, András Magyar, *C-band Adaptive Radio Direction Finding System*, Kommunikáció 2005., Budapest, Hungary, 27. October, 2005., pp. 347-359.
- [6] Rudolf Seller: Research on adaptive antenna systems, chapters 1-6.

Balázs Pándi:

Core Communications Network – an international overview

1. Definitions

American, British, German and French standards were considered to give a general overview. In order to be able to understand the systems, which are standard and operational in these NATO member countries on a system-level, it is important to clarify some key concepts. These concepts are not primarily concerned with the operation of the network, they provide common definitions for understanding the network-, service- and system-elements.

The concepts are the following:

Node: A communications centre, which is a fundamental component of the grid system, but is also capable of autonomous behavior. It integrates a switching centre, equipment providing transmission routes (stations), a radio receiver point, information protection devices, and allows users to access services provided by the system.

Grid system: A communications network in which a system of nodes interconnected in multiple directions provides the means of connecting command posts, communications centers or users to the network in order to form a common communications infrastructure.

Field coverage system: a stationary or field communications system installed at the field of operations, which in order to coordinate the troops, provides communications infrastructure for the commanders of the operation, the troops which carry out the operation, and the troops supporting and protecting the operation. With its application the means of connection is provided for various users at the entire area of application, thus all services provided by the network are available depending on access rights to users connected to the system.

Automatic routing: a service of digital systems, where during the selection of a predefined or random, physical or logical route (routing), the network automatically makes the requested connections using the communications and computer devices applied at the nodes.

2. System architecture

The examined systems apply a grid-structured field coverage network with the appropriate communications center density. This means that taking the features of the ground and the communication requirements into account, the nodes are placed considerably close to each other (approximately 15-30 kilo-

meters apart) on the field, and then connected to the neighboring nodes, thus forming a complex communications network. This system does not assume any axes as the analogue field core network did, because the nodes placed at the major heights of the area have the same capabilities, the lines connecting them have the same capacity, so all nodes of the network can accept the connection of communications centers of various command posts from tactical corps to even the General Staff. The installation and maintenance of the network belongs to the duties of the superior military unit (corps, division), all subordinate units only have to fulfill the requirements of connecting to the network.

This form signal corps support means that the subordinate units can focus their resources to fulfill their tasks, while the network is installed and maintained by the superior units. The size and composition of the network varies at individual armies, depending on the size of the area which needs to be covered by the network and the geographical conditions. This also means that the number of nodes needed to construct the network is also different in the various networks of the member countries. At an installation on an average terrain there is at least one a node at every 15-30 kilometers that command posts or mobile users can connect to.

The nodes in the network are usually connected via microwave radio-relay devices (the systems of some member countries also include sections using optical cables to connect a pair of nodes), and the stations use the frequency range specified by international (and NATO) standards. The structural-technical architecture of the nodes is quite similar at the systems of the various member countries, but the composition of the stations varies from case to case. For example, there are some member countries where the digital switching centre, the microwave radio-relay stations providing the transmission routes, and the radio receiver points are built in a separate station at the node communications centre. In other countries one or all communications centre parts of the node are integrated onto carrier vehicles, thus only one or two stations provide the connections for the node. Another common feature of these systems is the integrated digital services provided for the users. These are voice-, image-, data-, and multimedia-services, which integrate the computer and communications networks, regarding them as one system.

The tactical communications systems of NATO member countries, because of their digital nature, have modern ISDN¹ services, and allow the users to use the same kind of services on the field as they could use at their peace-time stations. The networks allow tactical units to connect to the grid system

¹ ISDN: Integrated Services Digital Network

through radio receiver points both automatically and by the manual connection of the personnel operating the node. In order to make this possible, families of radio devices have been developed and standardized, which are able to connect automatically (similarly to the working of cellular phone networks) to the network, and keep the connection alive while in motion with the nearest node, as a base station.

3. Connection of command posts to the network

The command posts of regiments and brigades usually connect to one (in some cases two) node through digital radio-relay channels, which end in the digital switching centers of the command posts. The command posts of divisions and corps connect to **two nodes** simultaneously through digital microwave-stations (and/or optical cables), with both nodes having the same capabilities and facilities. In other words both nodes provide complete services to the users connected to the command posts. This however requires that the primary and reserve command posts of the military units have the completely same architecture, and that the configuration of their communications devices match. The number of users connecting to the division and corps level command posts is usually between 50 and 100, but at the corps level command posts of some member countries this can even go up to a 150 users.

4. Priorities

The users of course have different rights to access the services provided by the network, therefore different priority categories have been introduced. There are usually three priority levels. There are users who, given their ranks (usually small number of commanding officers) can access the services of the network at **all times** and have access to services provided by other communications systems that connect to their networks (the networks of other member countries, civilian networks, NATO-network, etc.). This is the **top priority category ("A")**, the number of users belonging to this group usually amount to five to ten percent of all users. Users belonging to **second priority category ("B")** can be restricted in connecting to other networks, but can access all services in their own network. This category contains fifteen to twenty-five percent of all users. Thirty to forty-five percent of the users belong to the **third priority category ("C")**, and only have access to some services of the network. The rest of the users who **do not belong to any priority category** can usually only access the telephone service.

5. Network services

In terms of network services the systems satisfy the basic communication requirements of our time, integrate communications and computer networks

and their services. For example they provide the following communications and computer services:

- voice communication over open and secured lines
- videophone service
- point to point, or point to multiple points (conference), and broadcast connections
- fax communication over open and secured lines
- radio-control over digital phone
- digital switch center services, such as hotlines, call transferring-receiving, call switching, line tracing, caller id display, etc.
- access to network databases
- e-mail services, internet and intranet access
- operation of a military messaging system (MMHS)
- transfer of still and moving images, graphical interfaces

Beyond these services the nodes also provide a **radio receiver point service**, which allows mobile and fighting units, troops to be commanded via the switching centre from the telephones installed at the work stations. Units connected to these are also able to make a connection to any user through the network. The communications networks provide an opportunity for setting up a command and control supporting communications and computer system, and realizing a C4I² system that is automated, covers all areas of military command and control, and fulfils military requirements.

Besides this, it has also become a real requirement that the commanders and braches expect the same kind of services and facilities from the systems used to command the troops as the stationary networks provide at their peace time stations, offices.

6. Conclusions

The current core communications network of the mechanized corps does not fit the above requirements, thus it is **not efficient** to upgrade the existing system. The core field communications network and its command system should be set up, based upon these new foundations and principles, thus a system-based approach should be taken when designing the network.

² C4I= Command, Control, Communications, Computer, and Intelligence

References

- [1] Fekete, Karoly PhD: New possibilities in the field of WAN-WLAN military communications, „Communication 2004” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86441 5X, 15th September 2004
- [2] Mikita, János: A katonai infokommunikációs rendszerek fejlődésének főbb irányai, Bolyai Szemle, Vol 10/1, Budapest, ISSN 1416-1443, 2001
- [3] Munk, Sandor CsC: Information interoperability and communication, „Communication 2003” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86229 6 2, 15th October 2003
- [4] Rajnai, Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO tagországok kommunikációs rendszereinek tükrében, PhD dissertation, Zrínyi Miklós National Defence University, Budapest, 2001
- [5] Szöllősi, Sándor: Az új típusú haderő és a súlypont-átrendeződés kérdései a technikai struktúrában, „Communication 2003” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86229 6 2, 15th October 2003
- [6] Végh, Ferenc: A Magyar Honvédség a felkészüléstől a teljes interoperabilitásig, A NATO-tag Magyarország, Ministry of Foreign Affairs, Budapest, ISBN 963 7038 11 6, 1999

Szabó András

Kihívások a Magyar Honvédség elektronikus adatkezelő rendszereinek hitelesítése terén

A XX. század második felétől kezdődően az információ terjedése dinamikájában változott meg. Az utóbbi évtizedekben a tudomány és technikai fejlődés következtében a tudás értéke megnőtt, az információk összessége, megszerzése és birtoklása elsődleges céllá vált mind a magán, mind a kormányzati szektorban. Megnövekedett az igény a nagy mennyiségű adatok kezelésére, gyors feldolgozására és azok védelmére. Napjainkban az elektronikus úton történő adattárolás, felhasználás mértékével nincs arányban az információ, az információs hálózatok védelme. A védelmi szférában kiemelt figyelmet kell szentelni a kockázat mértékével arányos adatbiztonsági rendszer kialakítására, hiszen kis anyagi ráfordítással, nagy technikai tudással szinte bárki támadhat a hackerek, social engineer-ek eszköztárával. Az információ védelme, a folyamatos kommunikáció fenntartása döntő mértékben befolyásolja egy szervezet működőképességét, következőképpen eredményességét. Folyamatban van egy közös kormányzati intranet hálózat létrehozása (e-government, Elektronikus Kormányzati Gerinc - EKG), és a kormány a jövőben egyre nagyobb mértékben akarja felhasználni az internet és saját hálózata által nyújtotta lehetőségeket az állampolgárokkal történő kommunikációra (elektronikus választás, -ügyintézés, -oktatás és egyéb területeken) és a szervezeteken belüli információs műveletekhez. Ebben a hálózatban meg kell különböztetni a kormányzati szervek közti, továbbá a kormány és az állampolgár közti kommunikációt. Mindkettő kommunikációtól elvárjuk, hogy biztosított legyen a minősített adatok és az állampolgárok személyes adatainak védelme az illetéktelenektől.

A kormányzati szerveknek saját maguknak kell biztosítani hálózatuk védelmét, hiszen nem lehet a több száz kormányhivatalra, melyek különböző feladatot látnak el és eltérő elvárásaik vannak a hálózatukkal szemben, egységes felügyeletet állítani. Ezen szervezeteknek egyedül kell megoldaniuk a hozzáférések kezelését, naplózását, a jogosultságok nyomon követését. Fontosnak tartom hangsúlyozni, hogy annak ellenére, hogy minden szervnek különálló biztonsági felügyelete van, a koordinált munka szükséges ezen szervezetek eredményes működéséhez.

A NATO stratégiai víziója³ meghatározza a jövőre nézve, hogy milyen képességeket kell elérnünk. Ezek a döntés fölény, a koherens hatások és az összhaderőnemi telepíthető és fenntartható erők képessége. Az integrált

³ Strategic Vision: The Military Challenge – by NATO's Strategic commanders

logisztikai támogatás, a modul rendszer, az expedíciós műveletek mind megkövetelnek egyfajta hálózati képességet. A hálózat köti össze a felhasználókat a szükséges információkkal. Véleményem szerint, ez magas követelményt támaszt az információvédelem területén, hiszen a közös hálózatban csak a jogosultak számára szabad a szükséges információt elérhetővé tenni. A különböző nemzetek, hadseregek és haderőnemek más más követelményt és feladatokat támasztanak kommunikációs hálózataikkal szemben ez megoldhatatlanná teszi egy homogén hálózat kialakítását. A NATO elgondolás inkább a rendszerek rendszere elv megvalósulása lenne, ahol a különböző rendszerek kapcsolnánk össze egyfajta szövetségbe.

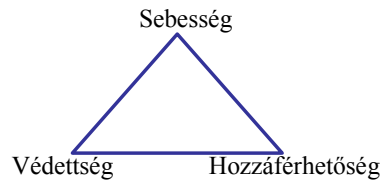
A hálózati képességek célja a parancsnoki munka segítése azzal, hogy a művelet teljes mélységében és spektrumában információt biztosít a parancsnoknak. A hálózatosított információs környezet lehetővé teszi, hogy a különböző hálózatokon tárolt információk a parancsnok előtt egyesüljenek.

A különböző helyekről összegyűjtött információkat logikusan rendeznünk és értékelnünk, továbbá "menedzselnünk" kell, hisz az első lépésben harcoló lövész parancsnoktól nem várhatjuk el, hogy az szükséges információk után a hálózaton "böngésszen", hanem módszeresen összeállított információ-csomagokat kell létrehoznunk számára. A Magyar Honvédségnek több minősített adatot kezelő hálózathoz is hozzá kell férnie (NATO, EU, EKG-n keresztül más szervezetekhez), bizonyos minősített adatokon végzett munkafeladatok nem oldhatóak meg stand-alone PC-ken. Ellenben az elektronikus minősített adatok hálózaton történő nyomon követése (melyik felhasználó másolta, törölte, módosította) komoly kihívás, nemcsak az informatika (hálózatfelügyelet, információvédelem) területén hanem például a személyügy, logisztika területén is, hisz a jogosultságok a beosztástól függenek, az állománytáblára legjobb rálátása pedig a személyügynek van.

Egy teljes körű vizsgálat szükséges a honvédségi információs rendszerekkel és képességekkel szemben támasztott követelményeinek felmérésére, mely figyelembe veszi a hatályos jogszabályokat, nemzetközi ajánlásokat, szabványokat.

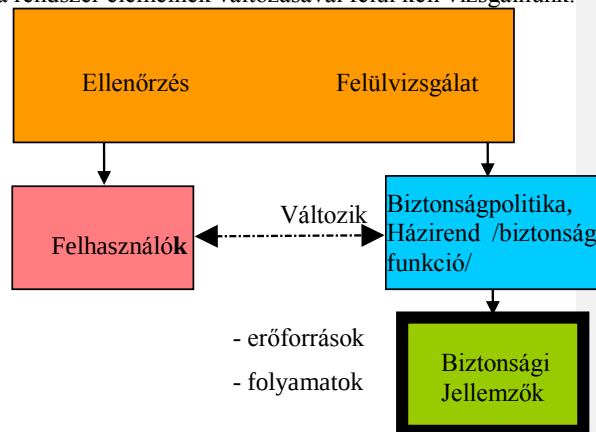
A jogi szabályzás törvényi szinten már kidolgozott a dokumentum és elektronikus információ védelem, elektronikus aláírás terén, erre alapuló technikai megvalósítás viszont még nincs teljes mértékben kidolgozva. Az Egyesült Államok Öböl háborús tapasztalatai azt mutatják, hogy az információs fölény nem képzelhető el hatékony információ biztonság nélkül. Ha bénítjuk az ellenség kommunikációs rendszerét, az egész hadsereg vezetés nélkül marad, hiszen megszüntetjük az érzékelő rendszer, a döntéshozó és a beavatkozó rendszerek közti folytonos kapcsolatot.

Az információ jellemzői: sebesség, védetség, hozzáférhetőség (1.ábra). E három tulajdonság egy képzeletbeli háromszög sarkain helyezkedik el, ha két tulajdonság megnövekszik a harmadik, következésképpen lecsökken.



1. ábra: Az információ jellemzői

A cél egy kompromisszumos megoldás kialakítása, mely eredményeképpen az elektronikus adatkezelő rendszer megfelel rendeltetésének. Például harcászati rendszereknél a sebesség a védetség előtt áll (ez lehet például a harctéren egy taktikai utasítás mely gyorsan célba kell érnie és elég a végrehajtás időtartama alatt védve lennie). Általános elvárásaink az elektronikus adatkezelő rendszerrel szemben: sértetlen, hiteles adatok szolgáltatása, a folytonos rendelkezésre állás és különböző szolgáltatások biztosítása. A rendszer biztonsági felügyelete végzi a felhasználó ellenőrzését, továbbá készíti a szervezet biztonsági házirendjét, amely a jelszavak kialakításának menetétől a tűzfal beállításán át a vírusvédelem eszközéig minden biztonsággal kapcsolatos problémához útmutatásul szolgál. A biztonsági felügyelet funkcióit a 2. ábra mutatja be. Láthatjuk, hogy a biztonsági szabályzatokat rendszeresen, a környezet és a rendszer elemeinek változásával felül kell vizsgálnunk.



2. ábra: A biztonsági felügyelet funkciói

A Nyilvános Kulcsú Infrastruktúra

A Nyilvános kulcsú Infrastruktúra (PKI, publikus kulcsú infrastruktúra) elméleti hátterét már a '70es években megalkották, megvalósításra mégis csak a '90es évek elején kezdték. Ennek oka a gyártók különböző, egymással csak részben kompatibilis hardver és szoftver eszközei, a rendszer elméleti hátterének bonyolultsága továbbá a megvalósítás komplexitása. A PKI többnyire csupán egy irányelv, megvalósítása többféle algoritmussal és módszerrel lehetséges. Ezen rendszerekben kriptográfiai eszközökkel valósítható meg az a biztonság, melyet a CIA követelmények (Confidentiality, Integrity, Availability) megfogalmaznak (képes biztosítani a kommunikáció bizalmasságát, sértetlenségét és a folytonos rendelkezésre állását). A PKI célja az, hogy egy az elektronika világában is működő „személyazonosítót” hozzunk létre, mellyel a felhasználókat egyértelműen, akár a törvény előtt is bizonyíthatóan fel tudjuk ismerni. Titkos kulcsú vagy szimmetrikus kriptográfiának nevezzük azt a rejtjelezést, amikor az üzenetet ugyanazzal a kulccsal titkosítjuk, és dekódoljuk. Ennek a módszernek fő hátránya, hogy az üzenettel együtt a kulcsot is el kell juttatni a címzettnek. Tehát a kulcscseréhez biztonságos csatornára van szükségünk.

A nyilvános kulcsú rendszerben a felek (felhasználók, szerverek) két kulccsal rendelkeznek, egy nyilvános és egy titkos kulccsal, továbbá közös algoritmust használnak. A nyilvános (public) kulcs bárki számára elérhető, a hálózaton vagy az Interneten névjegyzékben tárolható, a saját (privát) kulcs viszont kizárólag a felhasználó ismerheti, birtokolhatja (intelligens kártya, token, biometrikus azonosító). A két kulcs felhasználásával digitális aláírást lehet létrehozni, adatot lehet rejtjelezni, azonosításra alkalmas (nyilvános kulcsú hitelesítő rendszerekben a titkos kulccsal történő hitelesítő eljárást nevezzük digitális vagy más néven elektronikus aláírásnak). Általában az aszimmetrikus kódolást hibrid módon alkalmazzák a szimmetrikus kódolással. Ennek oka az aszimmetrikus rejtjelezés bonyolultsága, lassúsága. A gyakorlatban a kulcs cserére biztonságossá tételére használják a nyilvános kulcsú eljárásokat. Miután a kulcscsere megtörtént, a felhasználók valamilyen szimmetrikus rejtjelezésre váltanak. A nyilvános kulcsú infrastruktúra a nyilvános kulcsokat egyedi felhasználókhoz másnéven entitásokhoz köti, továbbá lehetővé teszi, hogy más felhasználók le tudják ellenőrizni az entitás és a felhasználó azonosságát.⁴ A nyilvános kulcs hitelességét egy harmadik fél biztosítja, úgy, hogy a felhasználónak egy tanúsítványt nyújt. Ez a tevékenységet a CA (Certification Authority) végzi, mint egy elektronikus közjegyző. A törvényi megfogalmazásban, mint tanúsítvány kibocsátó, vagy mint elektronikus közjegyző szervként hivatkoznak rá. Fontos megkülönböztetnünk a személyiségeket (identitá-

⁴ Bevezetés a Publikus (nyilvános) Kulcsú Technológiába és a U.S. Szövetségi Kormányzati PKI Infrastruktúrába - D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang 3. fejezete alapján

³ 2001. évi XXXV. törvény. az elektronikus aláírásról.

sok) a jogoktól, a kettő közti különbség az, hogy az identitás csak azt határozza meg, hogy a felhasználót azonosítani tudom, míg a jogok a már felismert felhasználók adathozzáféréseinek mértékét szabályozza. A PKI infrastruktúra nem más, mint alkalmazások, szolgáltatások, kommunikációs eszközök, továbbá szabályzatok és eljárások összessége, amely a felhasználók és a szolgáltató számára biztonságos adatátvitelt nyújt nyílt csatornákon keresztül. A PKI olyan alkalmazás infrastruktúrát nyújt, amellyel lehetővé válik a törvények által elfogadott kétkulcsú, harmadik személy általi hitelesítési és adatbiztosítási eljárások használata az elektronikus adatkezelő rendszerekben.

“3 A” követelmény

- *Authentication*: mely a személy azonosítását jelenti, a felhatalmazott felhasználók adatokhoz való hozzáférése. Megkülönböztetünk tulajdonos hozzáférést, csoportos hozzáférést.
- *Authorization*: jogok, felhasználói jogosultság ellenőrzése (egyszeri vagy állandó hozzáférés). Továbbá a felhasználó műveletvégzési jogosultságát jelenti: olvasás / írás / végrehajtás / törlés joga. A már azonosított felhasználó kérését megvizsgáljuk, hogy jogosult-e hozzáférni az adathoz, vagy fel lett-e hatalmazva az adott alkalmazás használatára.
- *Accounting*: mely folyamatos felhasználó ellenőrzését jelenti (hálózat monitorozás, biztonsági naplózás, tevékenység figyelemmel kísérése).
-

Magyarországon a 2001. évi XXXV. törvény szabályozza a digitális aláírások használatát. A törvényi szabályozás biztosítja számunkra az elektronikus aláírás felhasználhatóságát, meghatározza az elektronikus aláíráshoz szükséges szolgáltatások kialakításának szabályait, továbbá meghatározza a hatósági felügyeleti tevékenységeit. A törvény szerint három, a biztonsági minőségekben különböző aláírástípus létezik: elektronikus aláírás, a fokozott biztonságú elektronikus aláírás és a minősített elektronikus aláírás.⁵ Fokozott biztonságú elektronikus aláírás: olyan típusú elektronikus aláírás, amely az alábbi speciális követelményeknek megfelel:

- alkalmas a felhasználó egyén vagy alkalmazás azonosítására,
- egyedülállóan az aláíró személyéhez köthető,
- a dokumentum tartalmához kapcsolódik úgy, hogy az aláírást követően a dokumentumon végrehajtott módosítások érzékelhetők segítségével.

Minősített elektronikus aláírásnak nevezzük az olyan elektronikus aláírást, melyet az aláíró biztonságos aláírás-létrehozó eszközzel előállított aláírását

hitelesítés céljából elektronikus dokumentumhoz csatolja. Az elektronikus aláírás az informatikai rendszerekben kezelt adatokhoz kódolással előállított digitális jelsorozat, mely a dokumentum tartalmából és a felhasználó tulajdonában lévő, egyedi kulcsból matematikai eljárással áll elő, ezt csatoljuk a dokumentumhoz. Mivel az egyedi kulcsot csak a felhasználó ismeri, a dokumentum módosítása után végzett matematikai eljárás nem hozhatja ki ugyanazt az eredményt.

A PKI rendszer elemei⁶

- Tanúsítvány birtokos (felhasználó egyén, szervezet vagy alkalmazás, szerver)
- Tanúsító hatóság (Certification Authority; CA)
- Regisztrációs hatóság (RA)
- Digitális Idő- és Dátumbélyegzés Szolgáltató
- PKI adattár: név és címtár
- Visszavonási listák (CRL)
- Tanúsítvány kibocsájtó pont

A nyilvános kulcsú rejtjelezés előnyeit csak akkor használhatjuk ki, ha feltétel nélkül meg tudunk bízni a másik félben, ehhez szükséges a PKI bizalmi rendszere, mely biztosít a másik fél kulcsának hitelességéről. A CA által kiadott tanúsítvány igazolja, hogy a fél nyilvános kulcsa egyértelműen személyéhez köthető.

Az Elektronikus Közjegyző - CA feladata

A CA a létrehozott tanúsítványokra ráteszi a nevét és aláírja privát kulcsával, ezzel biztosítja a feleket arról, hogy ő bízik a felhasználóban. A CA nyilvános kulcsa segítségével lehet leellenőrizni a tanúsítvány valódiságát. A CA végzi a CRL lista generálását, frissítését (Certificate Revocation List).

A Regisztrációs Hatóság –RA feladata

A Regisztráció hatóságban megbízik a CA annak érdekében, hogy regisztrálja és tanúsítsa a felhasználók azonosságát. A 4. generációnál jelenik leginkább meg az RA rendszer adminisztrációs feladatköre.

- Felhasználó azonosítójának (kulcs) létrehozása, annak file-ban, tokenen vagy intelligens kártyán való tárolása, kártyamenedzsment (kiosztás, visszavonás, kulcs frissítés),
- Felhasználó létrehozása, törlése az adatbázisból,

⁶ Bevezetés a Publikus (nyilvános) Kulcsú Technológiába és a U.S. Szövetségi Kormányzati PKI Infrastruktúrába - D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang 3.1 fejezet alapján

- Kulcs és tanúsítvány kezelés.

A policy menedzsment kialakítása is az RA feladata, mely a kulcsmenedzsmentet és a rendszerelemek jogainak kezelését végzi. A tanúsítvány készítési kérelmeket az RA indítja a CA felé, majd az elkészült tanúsítványt az RA továbbítja a felhasználóknak. A tanúsítványok a nyilvános kulccsal mellékelődik.

A Visszavonási lista - CRL (Certificate Revocation List) feladata

Ez az adatbázis kezeli azon tanúsítványok listáját, melyek vissza lettek vonva (ok lehet, hogy a titkos kulcs kompromittálódott, már nem jogosult a felhasználó). Ez teszi naprakésszé az azonosítást. A CRL a PKI rendszer egyik alappillére, ha nincs megfelelő mértékben szabályozva, felügyelve, közvetett módon veszélyeztetjük a rendszert (mivel laza pórázon hagyjuk a felhasználókat, a kellenél nagyobb kockázatot vállalunk).

User agent

Ez egy alkalmazás, mely a felhasználó kéréseit, műveleteit végzi a kulcsokkal kapcsolatban. Elektronikus aláírás képzése, kódolás, dekódolás, hitelesítési eljárások, tanúsítvány igénylés a CA-tól, kulcsigénylés, visszavonás kérése.

Digitális Idő- és Dátumbélyegzés Szolgáltató

Időbélyeg szolgáltatás (Time Stamp – TS) lebonyolításáért felelős. Sok esetben szükséges a pontos datálás az időpont megállapításához (pl.: rendszernaplózás, hozzáférések, módosítások nyomon követése), ekkor időbélyeget használunk, mely a pontos dátumot is rögzíti kriptográfiai úton az elektronikus dokumentumon. Az időbélyeg logikai ok miatt csak digitális aláírás után helyezhető el a dokumentumon. Egy időbélyeg nem elegendő sok esetben, mivel csak azt határozza meg mi után keletkezett, ha szükséges a pontos időpont meghatározása, akkor ki kell alakítani a rendszerben egy időbélyeg tanúsító szervet, mely a hozzá elküldött időbélyeggel ellátott adatokat hitelesíti (saját időbélyegét ráhelyezi).

Hash eljárások

A dokumentumból egy matematikai művelet (egyirányú vagy más néven csapóajtó függvény) segítségével előállítunk egy olyan információt, melyből egyértelműen meghatározható az adat sértetlensége, valósága. Az eredmény az adat kivonata, ami az adat ujjlenyomatának tekinthető. Az adatkivonatot bármelyik fél elő tudja állítani ugyanabból az adatfolyamból, de szinte lehetetlen ugyanazt a kivonatot más adatfolyamból előállítani. Az eljárás törése csak a "nehéz" matematikai problémák megfejtésével lehetséges, vagy az implementáció hibáinak kihasználásával.

MH specifikus megvalósítás

A Magyar Honvédség sokrétű feladatainak ellátásához nagymértékben felhasználja informatikai hálózatát, a biztonsági intézkedéseknek garantálniuk kell azt, hogy a kritikus adatokhoz (Nemzeti, NATO minősített elektronikus dokumentumok) csak a megfelelő jogosultsági szinttel rendelkező személyek férhetnek. Az információkat egy elosztott környezetben kell védenünk - a stationer hálózat is kiterjed az egész országra, de a missziós feladatok összeköttetést igényelnek más országokkal, földrészekkel - ahol a felhasználók, erőforrások különböző helyeken és időben jelennek meg. Az MH speciális igényeinek megfelelően, egy biztonságos információvédelmi rendszer kialakítására van szükség, amely képes megfelelni a nemzetközi normáknak. „A védelmi infrastruktúra meghatározása: olyan rendszer mely PC-ből, kommunikációs hálózatokból, szoftverekből, alkalmazásokból, adattárakból továbbá olyan képességekkel áll, melyek az információ feldolgozás, tárolás és adatátvitel során szükségesek a védelmi felhasználók számára, békében és háborúban.”⁷

A világon a nyugati államok, különösen az Egyesült Államok támaszkodik informatikai rendszereire, fejleszti folyamatosan ezen a hálózatokat. Az NSA felmérése szerint 120 állam hadserege hozott létre informatikai támadó képességet, és számítanak ezen erők alkalmazására.

A Magyar Honvédségnek is lépést kell tartani a szövetségesek és más országok elektronikus adatkezelő rendszereivel egyrészt a kompatibilitás miatt, másrészt az esetleges felderítés elleni hathatós védelem céljából.

Fokozott figyelmet érdemel a elektronikus adatok, a számítógépes hálózatok védelme hiszen az MH hálózata melyet a vezetők, az alakulatok és az egyes katonák használnak fontos célpontja lehet egy külső támadónak, felforgató és terror csoportoknak. Hangsúlyoznom kell, hogy ugyan a MH - nak nincs ellenségképe, de az asszimetrikus fenyegetések növekedése párosulva az elektronikus hadviselés eszközeinek alacsony költségével, a tudásanyaghoz és az eszköztárhoz való könnyű hozzáféréssel (internet) komoly kockázatot jelenthetnek a jövőben.

A elektronikus információvédelem területén a hitelesítés, azonosítás és a letagadhatatlanság biztosításának kérdésével foglalkoztam. Céлом, hogy bebizonyítsam a PKI szükségességét a modern, elektronikus adatkezelő rendszerek biztonságának garantálásához. A PKI nem a védetség egyetlen eszköze, a rejtjelezés más módszerekkel is megoldható, de a hitelesség, visszautasíthatatlanság ezzel tökéletesen biztosítható. A PKI törvényileg elfogadott, a nemzeti és a szövetséges elvárásoknak is eleget tesz, a digitális aláírás révén hivatalossá teszi az elektronikus dokumentumokat, ezáltal a Honvédség elvá-

⁷ Information Security: Computer Attacks at Department of Defense Pose Increasing Risks(Chapter Report, 05/22/96, GAO/AIMD-96-84)

rásainak megfelel. Az Információs Tárcaközi Bizottság (ITB), mely 2002-től KIETB (Kormányzati Informatikai Egyeztető Tárcaközi Bizottság) fennhatósága alatt áll az állam adminisztrációs és közigazgatási területének informatikai fejlesztése, de a Magyar Honvédséggel kapcsolatos kérdésekkel nem foglalkozik. Mivel az elektronikus adatkezelő rendszerek a Honvédség minősített és nem minősített adatait kezelik, a hozzáférés kérdése merül fel elsősorban (melyik felhasználó, milyen szervezet, milyen okból férhet hozzá, továbbá ki felügyeli ezt). A Honvédség hálózatának NATO minősített adatkezelésre alkalmasnak kell lennie, továbbá képesnek kell lennie felkapcsolódni a szövetségesek hálózataira. A hálózat PKI alapú infrastruktúrával képes a kommunikáció bizalmasságának, integritásának, azonosításának és letagadhatatlanságának biztosítására. Figyelembe kell vennünk, hogy a Honvédség különböző elektronikus adatkezelő rendszerrel, különböző fejlettségű hálózattal rendelkezik, az új eszközöknél, eljárásoknál az alulról való kompatibilitás elvének kell érvényesülnie (pl.: az azonosítás terén is).

A későbbi fejlesztéseket könnyíti az, hogy PKI infrastruktúra a kereskedelmi forgalomba kapható termékekből felépíthető, így nem kell a relatív drága katonai fejlesztéseket, eszközöket többszörös áron megvásárolni. Hiszen a szervezeti egységek meleg tartalékolással, de a stacioner hálózatra csatlakoznak, szolgáltatásaikat a transzport hálózaton keresztül biztosítja a tábori felhasználók részére is. A civil szféra tapasztalatai, szakanyagai ugyancsak felhasználhatóak a rendszer további fejlesztése során, tehát a szükséges szellemi tőkével is rendelkezünk. A nyilvános kulcsú kriptográfiát rendkívül egyszerű egy felhasználó pár és egyetlen alkalmazás esetében bevezetni. A technológia egyszerűen méretezhető alkalmazások vagy néhány felhasználós hálózatok támogatására, de a közösség méretének növekedésével egyre nehezebbé válik a nyilvános kulcsok szétosztása és a hozzátartozó privát kulcs tulajdonosának monitorozása. A nyilvános kulcsú infrastruktúra műszaki, szervezeti és jogszabályi tényezők összessége, melyek egy decentralizált - sok telephellyel rendelkező, nagy személyi állományú - szervezet (mint az MH) számára számos követelményt támaszt. A nyilvános kulcsú kriptográfia szervezet szintű követelményei: a felhasználóknak szükségük van a nyilvános kulcsok kezeléséhez egy biztonsági infrastruktúra támogatására, mely kialakításához szükséges a HM információvédelmi szerveinek és a rendszer felügyeleti szervek együttműködésére. A PKI szervezeti igényeinek kielégítése céljából (Tanúsítvány kibocsátó szerv, Regisztrációs szerv, a visszavonási listák kezelése) szükséges lehet a HM Információvédelmi főosztály feladatainak bővítésére. Fontos említést tennem a lehetséges azonosító metódusokról. Egyes kiemelt helyeken biometrián alapuló azonosítás szükséges. Ilyen, szigorúbb biztonságot igénylő munkakörök: rendszergazdák, rendszeradminisztrátorok, információvédelmi szakemberek, a tanúsítvány kibocsátó szervet felügyelő szemé-

lyek, továbbá mindazon személyek, akik privilegizált jogokkal rendelkeznek a hálózatban.

Kontrolált intelligens kártya adminisztrációra van szükség, mivel egy kártya akár több alkalmazáshoz, beléptető rendszerhez tartozó kulcsot is tartalmazhat, azok kompromittálódása komoly kockázatot jelent.

A PKI alternatív felhasználása lehet a szoftver gyártó cégekkel történő kapcsolat fenntartása és a frissítések hitelesítése segítségével. A férgek, vírusok, spywarek korában fontos lehet a programok hitelesítése, a vírus irtó eszközök hálózaton történő frissítésének ellenőrzése, továbbá az esetleges hálózat figyelő programok felügyelete, azonosítása. A katonai alkalmazás miatt speciális igényeket is támasztunk a PKI rendszerrel szemben: a bevezetés egyszerűsége, a rendszer rugalmas kezelhetőség, a monitorozás és a hozzáférések naplózásának biztosítása. Fontos szempont, hogy más PKI termékekkel és szolgáltatókkal kompatibilis legyen (az Elektronikus Kormányzati Gerinccel és a NATO tagok rendszereivel), minimálisan függjön a gyártó cégtől, képes legyen támogatni az IAR rendszer, továbbá a szükséges alkalmazásokat (virtuális privát hálózatok, hozzáférés felügyelet, intelligens kártya kezelése).

Fontos a felelőségek tisztázása, a feladatok kiosztása a Honvédségen belül. A decentralizált hálózat megköveteli az egy pontról kezelt jogosultsági rendszert, ennek kialakításának helye a Honvédelmi Minisztériumban javasolt, hiszen itt egy kézben összpontosítva, pontosan regisztrálva lehet a jogosultságokat kiadni. A CA kialakítása a felsőszintű vezetés, tehát a HM információvédelmi osztályának feladata. Az RA feladata az, hogy az Elektronikus közjegyző számára ellenőrizze a tanúsítvány tartalmát, mivel ez a tevékenység az infrastruktúra biztosításához szükséges, a Híradó és Informatikai Parancsnokság (HIP) alárendeltségében kell üzemeltetni, így megvalósulna a hálózati és biztonsági felügyelet elkülönülése is.

A Központi Rejtjel Elosztó feladatköre kibővülne az intelligens kártyák regisztrációjával, továbbá a nyilvános, titkos kulcsok tárolásával.

Összefoglalás

A PKI egy fejlődő technológia, megvalósítására már több nyugati állam hadserege és kormánya tett lépéseket. A PKI-vel nap, mint nap találkozhat az egyéni felhasználó is, hiszen ez az alapja az elektronikus kereskedelemnek, a későbbiekben várhatóan az elektronikus ügyintézésnek is.

A rendszer előnyeit és hátrányait összevetve, arra az eredményre jutottam, hogy a PKI rendszerrel az azonosítás, hitelesítés és a letagadhatatlanság megfelelő mértékben biztosítható, de hangsúlyoznom kell, nincs tökéletes védelem. Hisz a biztonság mindig a rendszer leggyengébb pontjától függ, ami nem más mint az ember. A rendszerünk alkalmazhatja a legerősebb rejtjelező algoritmust, ha a felhasználó nem megbízható, kiszivárogtathatja az információt. A probléma az, hogy a felhasználók mindig megtalálják az útját, hogy hogyan

tudják leegyszerűsíteni a biztonsági rendszabályok követelményeit, éppen ezért tudatosítani kell az egyes felhasználókban, a biztonság az ő érdekük és felelősségük. Tudatosan nyitva hagytam a rendszer specifikus megvalósítás lehetőségeit, dolgozatomban nem kívántam összehasonlítani a cégek különböző szoftveres és hardveres eszközeit. Fontosnak tartom kiemelni azt, hogy az információvédelem területének fejlesztésére a Magyar Honvédségen belül igény lenne. A kutatások kicsiny része foglalkozik ezzel a témával, ellenben az információvédelem kérdésköre sok kiaknázatlan területet rejt.

Felhasznált irodalom:

- Sp800-32 Bevezetés a Publikus (nyilvános) Kulcsú Technológiába és a U.S. Szövetségi Kormányzati PKI Infrastruktúrába – D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang
http://www.ihm.hu/tarsadalom/kutatasok/PKI_ismertetes.pdf
- Commission Of The European Communities - Network and Information Security:Proposal for A European Policy Approach
- Magyar információs társadalom stratégia - Informatikai biztonsági részstratégia
- Decentralized IT: New Security Strategies - Gene Kim
- Kevin D. Mitnick – A megtévesztés művésze
- Kevin D. Mitnick – A behatolás művészete
- Nyilvános kulcsú titkosítás, digitális aláírás akadémiai hálózatokban - Pásztor Miklós
- Szöllősi Sándor: A megváltozott nemzetközi biztonságpolitikai környezet hatása a magyar honvédség info-kommunikációs rendszerére
- Information Security: Computer Attacks at Department of Defense Pose Increasing Risks(Chapter Report, 05/22/96, GAO/AIMD-96-84)

Bánfi Tibor

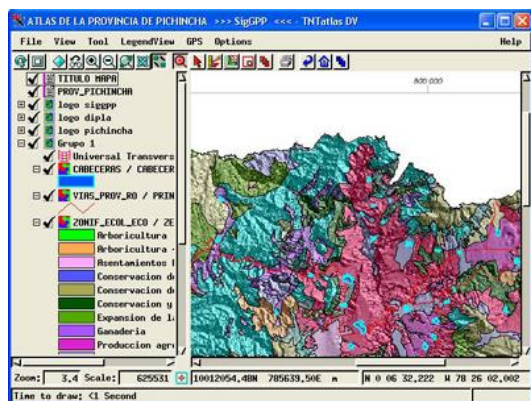
Digitális rendszerek alkalmazása a kínai katasztrófa elhárításban

„Kínai tapasztalatok szerint a nagy földrengések előtt a madarak abbahagyják dalukat, a lovak idegesek lesznek, a patkányok csoportosan menekülnek a földfelszínen.”

Röviden vázolni fogom a kínai földrengések elleni katasztrófa vezetés aktuális fejlesztési tendenciáit. Bemutatom az esetleges földrengések elleni védekezés modelljeit, a nyilvános oktatási és gyakorlati programokat, amelyek a katasztrófák megelőzését segítik elő, valamint azokat az eljárásokat próbálom vázolni, amelyekkel felbecsülhetjük a földrengések kockázatait, illetve a veszélyek tényezőit.

A számítástechnika rohamos fejlődésének köszönhetően a földrengés előrejelző berendezések is igen magas fokú fejlettséget értek el a XXI. században, melyek még több információt képesek biztosítani (rövid időn belül) a lehetséges veszélyforrásokról és kockázatokról.

Prezentációm utal a nagy terjedelmű állami tulajdonban lévő vállalkozásokra, amelyek a földrajzi információs rendszer (Geographical Information System, GIS), földi helyzet meghatározó rendszer (Global Positioning System, GPS) és a távérzékelő (Remote Sensing, RS)



Földrajzi információs rendszer (Geographical Information System, GIS)

Földi helyzet meghatározó rendszer
(Global Positioning System, GPS)



rendszer széleskörű építését szorgalmazták a városok részére. Szó esik a technikai fejlesztés építésének eljárásáról, amely magában foglalja az új digitális földrengés előrejelző berendezéseket a katasztrófa elhárítás rendszerén belül, az egységes módszereket, valamint az adatátvitelt és adat kommunikációt biztosító 3S rendszert.



Kína egy olyan ország a Földön, ahol a legtöbb ember „szenvet” a természet által okozott katasztrófa veszélyektől. Habár a katasztrófák enyhítésére igen jelentős lépéseket tettek, a veszélyforrások szinte kiapadhatatlanok, így a kihatások nagy gazdasági veszteségeket okoznak, amelyek Kína GDP-jéből 3-6 %-ot vonnak el (Kína GDP-je 2005-ben megközelítette a 1800 milliárd dollárt) és minden évben több mint ezren halnak meg. Kína rendkívül fontos feladatnak tartja a természeti katasztrófák veszélyeinek csökkentését. 1989-ben az Európai Unió is támogatta a Nemzetközi Természeti Katasztrófa Csökkentés (IDNDR) című programot. A Kínai Kormány nagy hangsúlyt fektetett olyan különböző programokba, amelyek támogatják mind a természeti katasztrófák, mind pedig a civilizációs katasztrófák által okozott veszélyforrások megelőzését és megakadályozását.

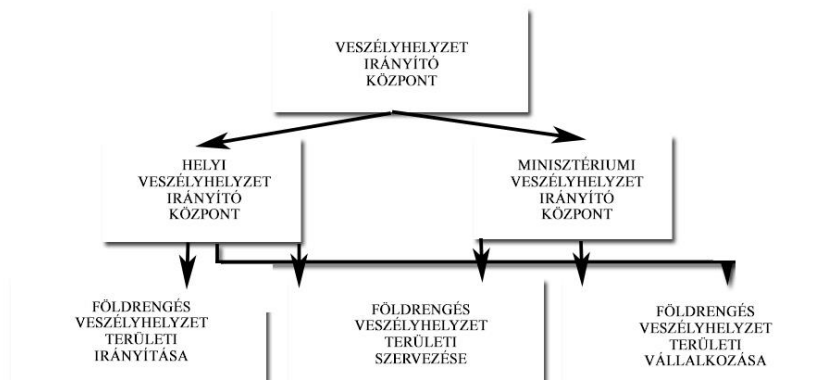
A sajátos földrajzi fekvése miatt Kínában magas a földrengés veszély kockázata – mivel a híres Csendes-óceáni lemez találkozik a Himalája lemezével. A földrengés veszély negatívan befolyásolja ennek az országnak a fenntartható fejlődését. A kormány a '70-es évek óta fontosnak tartja, hogy olyan lépéseket tegyenek, amelyekkel csökkenteni tudják a földrengés veszélyének kockázatait. Az elmúlt években látványos eredményeket értek el ezeken a területeken. A statisztikák szerint szinte minden nagyobb város és állami vállalkozás felállította a saját katasztrófa irányítási rendszerét. Néhány város, ami olyan helyen fekszik, ahol magas a földrengés veszélyének kockázata minden évben modellezett körülmények között gyakorolja a mentést és a gyors helyreállítást.

Vezetési modell

Kínában a vezetési rendszer felépítési modellje hasonlít egy piramishoz. Csúcson a Veszélyhelyzet Irányító Központ, a Kínai Állam Kormány és a

Kínai Szeizmológiai Iroda helyezkedik el, ezek a legfelsőbb szervek. Másodlagos irányítóként a minisztériumok és a területi kormányok vesznek részt a munkában, a helyi kormányok harmadikként csatlakoznak, illetve más szervezetek vagy vállalkozások vannak a piramis lábánál. (A felépítést az első ábra mutatja).

A központi politikai rendszer valamint a veszélyhelyzet irányító központ képes arra, hogy a városokat megfelelően felkészítse, a forrásokat központilag helyesen mozgósítsa, illetve megtegye mindazokat a lépéseket, amelyekkel elősegíthetik a katasztrófa-elhárítást vagy az esetleges mentési feladatokat.



1. ábra: Vezetési rendszer felépítési modellje

A veszélyhelyzet irányító központ

- ad ki közvetlen utasításokat;
- felügyeli és koordinálja a területi, illetve a helyi mentési tevékenységeket a földrengés okozta súlyos veszteségek által elszenvedett területeken.

A helyi és a minisztériumi veszélyhelyzet irányító központ

- eszközökkel látja el a katasztrófavédelem szerveit a közigazgatási területein belül;
- követik a központ utasításait;
- segítik a kutatási, mentési és a katasztrófa-elhárítási feladatok végrehajtását (főként a nagyobb régiókban).

A földrengés veszélyhelyzet területi irányító önkormányzata, szervezetei és vállalkozásai

- felügyelik a mezőgazdaságban és az iparban elszenvedett veszteségeket;
- a polgári lakosságot ellátják az alapvető szükségletekkel (ivóvíz, élelmiszer, stb.);
- folyamatosan tájékoztatják a felsőbb központokat az:
 - eseményekről;
 - eltűntekről, valamint a;
 - szeizmikus helyzetről.

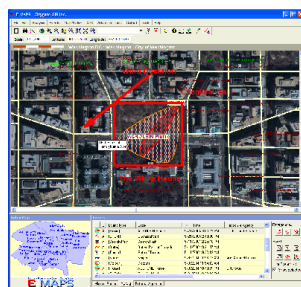
Alapvető információs rendszerek a földrengés által okozott katasztrófák mérsékléséhez

A digitális földrengés-megfigyelő hálózat segít a kínai kormánynak a földrengések előrejelzésében, így megelőzhetőek a katasztrófák és azok potenciális hatásai a térségben. Hatékonyabbá válik a közbiztonság és növekszik a kínai lakosság életminősége.

A kiváló digitális térképészet az 1990-as évektől kezdődően kiindulópontként szolgál az építkezésekhez. Napjainkban a Kínai Kormány nagy jelentőséget fordít a tudományos és technológiai fejlesztésekre, mint a földrengés által okozott katasztrófák mérsékléseinek alapjául szolgáló információs rendszerekre. A következő években a „Digitális Föld” („Digital Earth”)⁸ és a Kínai Nemzeti Információs Infrastruktúra (China’s National Information Infrastructure; CNII)⁹ projektet indítják el. Ez a rendszer foglalkozik a földrengések mérséklésére szolgáló információk integrálásával, olyan digitális geológiai térképekkel, melyek méretaránya 1:50,000, 1:250,000 és 1:1,000,000 országrészenként megosztva. Tartalmazza a geológiai struktúrákat, a földrengés történelmet, illetve magában foglalja a népesség és az épületek, építmények arányos elosztását. Minden területi székhelyű városoknak, illetve nagyobb városoknak, amelyek meghaladják az egymillió főnyi lakosságot egyéni digitális geológiai és információs rendszerrel kell rendelkeznie, amelyek térképeinek méretaránya 1:25,000, 1:10,000, 1:5,000. A különböző egyéb speciális térképek még több információt nyújthatnak. Azok a városok, ahol az összlakosság létszáma eléri az 500,000 főt, saját maguk alapozzák meg az információs rendszereiket. Ezek a rendszerek képesek előre jelezni a földrengést, illetve kielemezni a különböző veszélyforrásokat. Magukba foglalják az infrastrukturális információkat, a vízellátási hálózatot, az energia ellátást, a telekommunikációs hálózatot, a közlekedési hálózatot, illetve a lakosság és épületek elosztását a város területén belül. A 2. ábra tipikus példával ábrázolja a szervezési és mentési tervező rendszert (város nagyságú), ez a rendszer az aktuálisan alkalmazott veszélyhelyzet kezelésre szolgál.

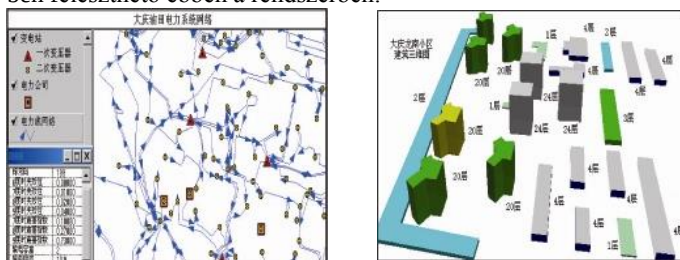
⁸ <http://www.digitalearth.gov/>

⁹ http://www.trp.hku.hk/papers/2001/china_convergence.pdf



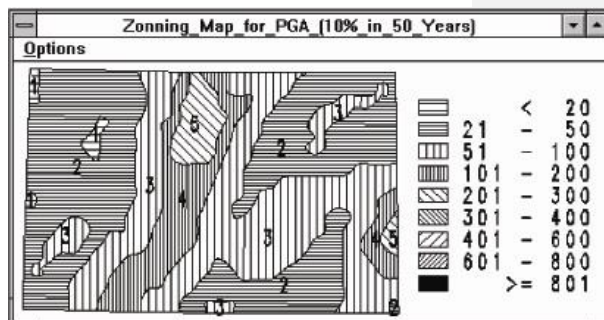
2. ábra: Szervezési és mentési információs tervező rendszer

A hatalmas kiépített infrastrukturális adatbázis mellett mindig új eredményeket adnak a már meglévő információkhoz a földrengést kutató mérnökök. Ilyenek például a földrengés kockázatának analízis elmélete, az anti-szeizmikus kritériumok vagy kódok, újabb tapasztalatok a katasztrófát megelőző, illetve katasztrófák utáni veszélyhelyzet-elhárításról. A 4. ábra az első digitális térképet ábrázolja, amely kiindulópontként szolgál a földrengés valószínű kockázatának lehetséges analízisére (GIS 1994). Az új számítógépek már alkalmazzák ezeket a rendszereket és az elkövetkezendő évtizedekben még nagyobb áttöréseket várnak ezeken a tudományos területeken. Például a földrengés okozta katasztrófa csökkentésének egyre fejlődő platformul¹⁰ szolgál a földrajzi információs rendszer, a földrengés xveszélyének vizsgálat analízis modellje valamint a földrengés okozta veszteség értékelési modellje könnyedén és időben felelthető ebben a rendszerben.



3. ábra Infrastrukturális információs adatok a földrengés katasztrófa-elhárításban

¹⁰ Platform: Jól behatárolható jellemzőkkel rendelkező [számítógépes hardver](#)- vagy [szoftver](#)-környezet. Rendszer platform a [hardver](#) és a [szoftver](#) kombinációja, amely meghatározza, hogy az adott [számítógépen](#) milyen egyéb [szoftverek](#) használhatók.



4. ábra Egy földrengési övezet térképe (GIS; Észak-Kínában)

Kína területe hatalmas (9.6 millió km²), így nagy különbségek vannak a fejlesztendő területeken belül is.¹¹ Lehetetlen felépíteni az információs adatbázis alapjait minden város számára. Szinte minden alapot a szeizmikus tudományra és technológia szintjeire lehet tenni, valamint az államgazdasági képességéhez mérni. A kormány nagy figyelmet és sok pénzt fordít a veszélyeztetett városok területeinek készenlétére és a veszélyforrások csökkentésére.

A kormány számos training programot indított el azért, hogy felkészítse az embereket a földrengés veszéllyel szemben és a kockázat csökkentésének teendőire. Mivel Kínában a minisztérium felelős a földrengés okozta katasztrófa elleni felkészültségért, és ahogyan azt „a földrengés okozta katasztrófa enyhítése és az ellene való védekezés” törvénye kimondja minden önkormányzat és néhány fontosabb állami kézben lévő vállalat létrehozta a saját földrengés veszély helyzetre szóló akció tervét összhangban környezetük földrengés veszélyeztetettségével.

¹¹ A legtöbb K+F intézet (80 %) a tartományi vagy városi kormányzatok irányítása alatt működik. A kutatók, mérnökök és technikusok létszáma megközelíti a 20 millió főt, de területi eloszlásban – Peking, Shanghai és Tienjin városokban az összes 20%-ka dolgozik - nagy a szórás, így az összehangolt munka és a hálózati szemlélet bevezetése került előtérbe az utóbbi években. Szoros együttműködés kialakítására törekszik az államtanács a helyi, járási kormányzatokkal az erőforrások koncentrálásának érdekében. Emellett integrált irányítási rendszer kiépítésével kívánja elősegíteni az állami vezetés a regionális ipari-egyetemi-kutatóintézeti együttműködést. <http://www.nkth.gov.hu/main.php?folderID=1943&articleID=4813&ctag=articlist&id=1> 2006. június 27.

Minden évben nagyarányú - hosszasan már előre megrendezett földrengés katasztrófát szimulálva - a polgári lakossággal közösen gyakorlatokat hajtanak végre. A Kínai Köztársaságban 1998-ban alkották meg a földrengés által okozott katasztrófák elleni védekezés törvényét.



2002 júliusában rendeztek Tashan-ban egy földrengés katasztrófa-elhárítási gyakorlatot

(képek: <http://www.sina.com>)

Az emberek földrengés veszéllyel szembeni elővigyázatosságát elősegítő projekt a következőt foglalja magába:

- törvényhozások a földrengések elleni védekezésre, illetve megelőzésre;
- a nyilvánosság számára biztosítani az alapvető információkat a földrengésről és azok veszélyeiről;
- széles körben ismertetni a földrengés által okozott balesetek elkerülési lehetőségeit;
- megfigyelő hálózatok építése, előrejelző berendezések telepítése a súlyosan veszélyeztetett zónákban;
- tervek készítése a speciális körülmények bekövetkeztére;
- szervezetek jelenléte, felmérések és látogatások a veszélyeztetett területek lakóházaiban (közvetlen lakossági tájékoztatás);
- tervezés és gyakorlati programok a földrengés elleni katasztrófák készenlétére, a különböző szervezetek folyamatos tájékoztatása, veszélyhelyzet kezelési, mentési és vezetési információk;
- olyan, a földrengés által okozott katasztrófa elleni rendszerek építése, valamint folyamatos fejlesztése, amely biztosítja az emberi életek, illetve a lakosság birtokainak és vagyonértékeinek megővését.

A jövőben három nagy jelentőségű rendszert kívánnak felállítani és kiépíteni Kínában:

- a katasztrófa-elhárítás folyamatos készenléti állapotának elősegítését biztosító rendszert;
- földrengés megfigyelő és előrejelző rendszert;
- megelőző és veszélyhelyzet reagálási/mentési rendszert.

Az időszakos gyakorlatok kimutatták, hogy az eljárási módok hatásosnak bizonyultak az emberek illetve a közösségek köreiből és ezzel csökkenteni tudták (és a jövőben még inkább lehetséges) a katasztrófák által bekövetkezett sérülések számát.

Kína igyekszik minimumra csökkenteni a földrengések következményeit (Song Rui-xiang, a Kínai Szeizmológiai Hivatal elnöke)

Song Rui-xiang leszögezte¹²: Kínában a központi kormány irányítása alatt minden városban földrengés-megfigyelő és segélynyújtási hálózat alakul ki, hogy az esetleges földrengések esetén minimumra csökkentsék a bekövetkező kár nagyságát.

Fontos intézkedések közé tartozik, hogy 2 milliárd 700 millió yuan¹³-ra fordítással digitális szeizmológiai hálózatot létesítenek. Segítségével tájékozódnak a világ bármely pontján, kiváltképpen az ország 9 millió 600 ezer négyzetkilométer szárazföldi és 3 millió négyzetkilométernyi tengeri területének bármely részén történő földrengésről. Ezzel megerősödött az ország déli és északi pontján működő gyenge, és a főváros környékén egyébként erősnek tartott földrengés-megfigyelés. Felgyorsították a reagáló-képességüket és a beavatkozó műveletek megszervezését is. 2000-ben megszervezték Kínában az első 200 szakemberből és orvusból álló földrengési segélynyújtó csapatot, amely nemcsak hazai földrengések esetén végeznek segítségnyújtást, mint például Xinjiang Uygur Autonóm területen, hanem tavalyi például Algériában és Iránban is. Az eredmény kétségtelen, ezért tartományi szinten is szerveznek majd hasonló rendeltetésű csoportokat. Az ország nyugati részén szeretnének két csoportot létrehozni. Ott jóval gyakoribbak a földrengések, és a nagy távolságok mindig nagy idővesztést okoznak. A földrengési csoportok mellett megfelelő figyelmet fordítanak arra, hogy minden nagyvárosban szaktanfolyamokat szervezzenek a tűzoltóság és a bányászati mentőcsoportok tagjainak, hogy szükség esetén ők is be tudjanak kapcsolódni a mentésbe. A csoportok megszervezése mellett minden városban szerveznek önkéntes mentőcsoportokat is, tagjaikat szaktanfolyamokon képezik ki, de ismeretterjesztő munkát is végeznek, hogy a lakosság is tájékozottabb legyen, és ismerje meg a meneküléshez szükséges tudnivalókat. Song Rui-xiang, a Kínai Szeizmológiai Hivatal elnöke megállapította, hogy a földrengések következményeinek csökkentésére

¹² Forrás: <http://hu.chinabroadcast.cn/1/2004/09/20/2@19137.htm> [2006. 05. 12]

¹³ Kb. 87. 472. 700 USD / 19 milliárd HUF

igen fontos szerep jut a biztosítótársaságoknak is. Kínában jelenleg szervezés alatt áll egy olyan biztosítótársaság létesítése, amely csökkenti a bajbajutottak kárát. Az érintett kormányzati intézmények a pénzügyi szervek és az adóhivatal bevonásával tanácskoznak e rendszer alakításán. A munkába be lehet vonni a társadalmi szerveket is.

Technikai eljárásmodok a katasztrófavezetésben¹⁴

A nemzeti gazdaságnak a virágzó és gyarapodó városok érdekeit figyelembe véve garanciát kell, hogy vállaljon a fenntartható fejlesztésekre és a megfelelő szociális haladásra és ezeket biztosítani is kell. Kína 1949-ben különös katasztrófális földrengés áldozatává vált, amelyben rengeteg ember vesztette életét és nagy gazdasági veszteséget is okozott. A magas színvonalú új eljárások mind a tudományban és mind a technológiában kihangsúlyozzák, hogy milyen rendszereket érdemes a katasztrófa-elhárítás számára kifejleszteni és építeni. Kínában jelenleg majdnem minden technikai lépés fellelhető.

Beijingben (Peking) a kormány „A földrengés által okozott katasztrófa-csökkentési,- illetve készenléti tervek a főváros köreiben” címmel beindította rendszeres demonstrációval az előrejelző és veszélyhelyzet kezelő rendszerek kiépítését. Ez a projekt három rendszer alatt fog futni:

- földrengés megfigyelő és előrejelző rendszer;
- hirtelen veszélyhelyzeti reagálási rendszer;
- propaganda és oktatási rendszer;

Az első két rendszer alatt alkalmazott a:

- fejlett digitális szeizmográf;
- digitális földrengés megfigyelő;
- földrengés adatgyűjtemény és analízis technika;
- 3S technológia (GIS, GPS, RS).

A harmadik rendszer alapjául szolgálnak az új generációs számítógépek fejlett technológiája, azon belül a különböző internetes oldalak felületei, tartalmai.

A mai orosz, illetve amerikai műholdak segítségével is már előre lehet jelezni a különböző földrengéseket és ezáltal is nagymértékben lehet csökkenteni a katasztrófák valószínűségét. A biztonság érdekében az Európai Űrügynökség¹⁵ Envisat nevű műholdja, percenként hat giga-byte mennyiségű adatot gyűjt össze és naponta négyszer el is küldi a szárazföldi megfigyelőközpontba, ahol

¹⁴ Technikai és információs háttér. A katasztrófa elhárításra szolgáló információs hálózatok, rendszerek tervezése, telepítése valamint alkalmazása.

¹⁵ European Space Agency, ESA

egy kilenc méteres antenna segítségével fogják a jeleket. A műhold részletes bontásban ad képet Hongkong 2500 km-es körzetéről, vagy 10 ezer négyzetkilométeres teljes lefedettséget ad Dél-Kínáról, Indonéziáról, Koreáról és Japán déli részéről. Jelenleg a Hongkongi Egyetem Űr- és Földkutatási Tudományos Intézetében a szakemberek tesztelik a rendszert, amely, ha minden jól megy, jövő évtől lép szolgálatba. A kínai szárazföldön és Ázsia egyéb területein is rendszeresen áradások, tájfunok söpörnek végig, gyakoriak a földrengések, de az új megfigyelőrendszer előre jelzi az olyan cunamikát is, mint amilyen pusztított az Indonéz szigetvilágban. A kutatóintézet igazgatója elmondta, hogy az új módszer nagy előnye, hogy több időt ad a katasztrófa előtti felkészülésre és a lakosság kitelepítésére. Ugyanis az eddigi műholdak csak akkor jelezték a bajt, amikor már a földrengés, vagy tájfun láthatóvá vált. A legújabb fejlesztések segítségével azonban már az árulkodó jeleket is rögzíteni tudják a műholdak, amiből olvasni tudnak a kutatók és az őket segítő egyetemisták, akik az adatok elemzésével foglalkoznak majd. Eközben egy német és indonéz tudósokból álló csoport, a tengerszinten végzett méréseket helyezi előtérbe. Szenzorokkal ellátott bójákat telepítenek a tengerre, amelyek mérési adatai szintén műholdas közvetítéssel jutnak el a szumátrai megfigyelőbázisra. A bóják tízpercenként küldenek információkat a tengerről, az esetleges víz alatti földrengésekről és cunamikról. Az év végéig kiépített rendszer veszély esetén automatikusan riasztja majd a hatóságokat SMS-ben, e-mailben, vagy faxon.¹⁶



Olyan *speciális szakcsapatokat* hoztak létre, akik *helyi szinten* figyelemmel kísérik a nap 24 órájában a különböző földrengés jelenségeket. Említést tettem arról, hogy vannak olyan jogszabályok, amelyek különböző területen szabályozzák az építkezések folyamatait, illetve maga a területi foglaltságot.

¹⁶ Forrás: http://www.radio.hu/index.php?cikk_id=157204&rid=PT1RTTRFVE0 = [2006. 05. 11]

Ezeknek a csapatoknak az egyik fő feladata, hogy a nem megfelelő építkezéseket felkutassák és súlyos pénzbüntetési bírságokat is kiszabadhatnak ilyen eseteknél.

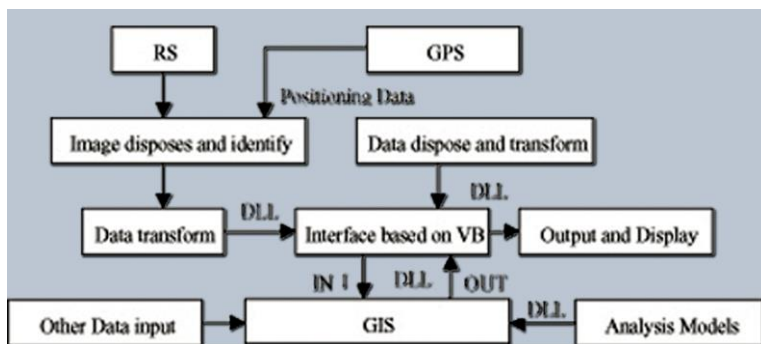


Kínai Speciális Mentő-csapatok



Problémák és megoldások a földrengés által okozott katasztrófa elhárítás vezetési rendszerének építésében.

A katasztrófa elhárítás vezetési rendszere hatalmas kapacitással kell, hogy bírjon, amely leginkább a pénzügyi erőforrásokban és az információkban merül ki. A 3S technika bizonyítja, hogy mennyire fontosak a szinte már tökéletesített programok ezekben a rendszerekben. A lehetséges különbségek a 3S rendszer adattípusai között, az adat átvitel a 3S rendszer és más adatok között, valamint a rendszer integrálása más rendszerekhez kulcsfontosságú probléma. Az 5. ábra vázolja egy kisebb rendszer megoldási lehetőségét.



5. ábra Egy egyszerű 3S integrált modell

Ez a rendszer a GIS magjának egyesítése, tartalmaz minden analízis modellt. Az adatokat az RS és GPS számára összekapcsolja a DLL (Dynamic Link Library - Dinamikus Csatolású Könyvtár) technikával, valamint a Visual Basic¹⁷ alapjainak integrálásával.

Konklúzió

Ezek a rendszerek hosszútávon sikeresnek bizonyulhatnak és mind a társadalom, mind pedig a katasztrófa vezetés előnyére válhatnak. Bár digitális technikákat alkalmazva a természeti csapások elleni védekezéshez igen nagy befektetést jelent az állam részére, nagy energiát, pénzt és technikai felszerelést (pl. rozsdálló és tartós szenzorokat) jelent.

Internetes források, tanulmányok

1. Lili Xie, et al (2000): Digital disaster reduction system. Journal of natural disasters, Vol. 9, No.2, 2000.
2. Yafeng Shi, et al (1992): Digital disaster analysis, strategy and countermeasure against disaster in china. The Division of Earth Sciences of China Academy of Science, Hubei Publishing house of science and technology , 1992.
3. Yongxiang Lu (1999): Building up the Digital Earth Together, Sharing Global Data Resources Each Other. Proceedings of the International Symposium on Digital Earth, Science Press, 1999.
4. Guanhua Xu (1999): Building the „Digital Earth”, Promoting China’s and Global Sustainable Development. Proceedings of the International Symposium on Digital Earth, Science Press, 1999.
5. Aiping Tang, Xiabin Tao, et al (2000): Digital System for Natural Disaster Mitigation in China. Prague, Republic of Czech: International conference of 30th Urban data management symposium (UDMS2000), 2000.
6. www.fema.gov
7. www.rand.org
8. www.sina.com
9. library.thinkquest.org/03oct/00904/reng.htm
10. www.radio.hu/index.php?cikk_id=157204&rid=PT1RTTRFVE0=
11. hu.chinabroadcast.cn/1/2004/09/20/2@19137.htm
12. www.mapasia.org/2003/index.htm
13. www.gisdevelopment.net/application/natural_hazards/floods/pdf/ma03032.pdf
14. www.undp.org/cu/eventos/espacial/MapAsia%202003.pdf

¹⁷ A Visual Basic (VB) a Microsoft cég által kifejlesztett programozási nyelv illetve fejlesztői környezet. A BASIC programozási nyelven alapul.

15. www-tem.jrc.it/PDF_publicis/2003/Stibig_EUR_2003_full.pdf
16. www.apecenergy.org.au/assets/documents/apecinternet/EarthquakeDisaster20050930114041.pdf

Képek

1. www.pocketpcmag.com
2. www.microimages.com
3. www.space.eads.net
4. www2.chinadaily.com.cn www2.chinadaily.com.cn
5. news.bbc.co.uk
6. www.humanrights-china.org

Máté József pv. alezredes

Monitoring és Lakossági Riasztó Rendszer megvalósítása

Előzmények:

A 96/82 EK SEVESO II Tanácsi Irányelv az EU jogharmonizáció környezetvédelmi fejezetének illesztéseként került implementálásra a „A katasztrófák elleni védekezés irányításáról és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről” szóló 1999. évi LXXXIV. törvény IV. fejezetében, valamint „A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről” szóló 2/2001. (I.17.) Korm. rendeletben foglaltak alapján.

A SEVESO II Irányelv megteremtését jelentős veszélyes ipari balesetek súlyos következményei indukálták, mint:

- 1974 Flixborough, Anglia – ciklohexán,
- 1976 Seveso, Olaszország – dioxin
- 1986 Bazel, Svájc – peszticid szabadba jutása

Az Irányelv 2002-re vonatkozó további szigorítását motiválták:

- 2000 Baia Mare, Románia, cianid szennyezés
- 2000 Enshede, Hollandia, pirotechnikai anyagok robbanása

A példaként felsorolt események veszélyes anyagok okozta rendkívül súlyos baleseti következményekkel jártak, amelyek az emberi életben, a természetben, a környezetben jelentős károkat, veszteségeket okoztak. Az előzőek alapján a SEVESO II Irányelv magyarországi bevezetése a környezetvédelmi fejezet „problémás” részét képezte. Az EU Bizottság a magyar fél által a tárgyban benyújtott derogációs kérelmet „nem tárgyalhatónak” tartotta. A hosszú egyeztetések után a derogáció visszavonásával, kiegészítő információk megadásával SEVESO II teljesítését elfogadta. A fent említett törvényekben előírt feladatoknak való megfelelés érdekében az Országos Katasztrófavédelmi Főigazgatóság, kezdeményezte egy olyan integrált rendszer (meteorológiai és vegyi monitoring, valamint lakossági riasztási rendszer (MoLaRi)) kiépítését, amely teljes mértékben megfelel a kor társadalmi és technikai elvárásainak.

A rendszer három fő részből épül fel:

- vegyi monitoring és meteorológiai végpontok rendszere
- kommunikációs és informatikai-adatátviteli rendszer
- lakossági riasztó és tájékoztató rendszer

A monitoring és a lakossági riasztó tájékoztató rendszer kiépítése 21 üzem környezetében valósul meg. A rendszer 9 megyét (Borsod-Abaúj-Zemplén,

Csongrád, Fejér, Győr – Moson - Sopron, Komárom - Esztergom, Szabolcs – Szatmár - Bereg, Tolna, Veszprém, Zala) és a fővárost érinti.

Vegyí monitoring és meteorológiai végpontok rendszere

A monitoring rendszer a veszélyes ipari üzem területén (a veszélyeztetett irányokban) és a veszélyeztetett települések határában kerül telepítésre. A vegyi monitoring rendszer vonatkozásában veszélyes ipari üzemként átlagosan 4 meteorológiai állomással és gázérzékelőkkel is felszerelt, valamint 14 kizárólag gázérzékelőkkel ellátott mérési pont kerül telepítésre. A monitoring rendszer mérőszondái által mért adatok a veszélyes ipari üzemből elhelyezett gyűjtőközpontokban (helyi központ) folyamatosan kerülnek gyűjtésre, melyek az országos központban kerülnek feldolgozásra, ahonnan az információ az érintett megyei (fővárosi) katasztrófavédelmi (polgári védelmi) igazgatóság ügyeletére kerülnek továbbításra. A veszélyes koncentráció elérése után - a veszélyes ipari üzemmel történő egyeztetést követően - történik a lakosság riasztása. A monitoring végpont veszélyes ipari üzemből való elhelyezése és a riasztási küszöbök megfelelő beállítása biztosítja, hogy csak a tényleges súlyos ipari baleset kerüljön jelzésre. A monitoring alrendszer lakóterületen elhelyezendő mérőberendezései a veszélyes ipari üzem kerítésénél a rendszer által már korábban jelzett gázfelhő lakott területen való megjelenését, felhígulását mutatja. Fő rendeltetése adatok szolgáltatása a települési lakosságvédelmi intézkedések kellő időben való bevezetéséhez.

A mérőállomás

Az alrendszer meteorológiai és vegyi monitoring mérőállomása - *a veszélyhelyzeti felderítő gépjárművek felszerelése* - a TVS-3 monitoring állomás. A TVS-3 intelligens vegyi és nukleáris monitoring állomás - a meteorológiai jellemzők ismeretében - alkalmas egy adott terület, objektum vegyi és nukleáris jellemzőinek folyamatos és önálló ellenőrzésére, az esetleges veszélyeztető hatás korai felderítésére, a helyzet értékelésére, és a lakosság életét és egészségét veszélyeztető anyagok terjedésének meghatározására. A TVS-3 monitoring állomás alkalmas a fenti adatok összesítésére, tárolására és továbbítására is. A TVS-3 meteorológiai érzékelő részei: szélirány, szélsébség, hőmérsékletmérők két magassági szinten, talajhőmérséklet, relatív páratartalom mérő. A környezetre veszélyes anyagok koncentrációjának mérésére kifejlesztett GTI intelligens gáztávadók egyszerre négy gáz mérését teszik lehetővé. Az állomáshoz csatlakoztatható a BNS-98 típusú dózisteljesítmény távadó is.



a TVS 3 állomás (minta)

A rendszer kialakításának főbb szempontjai

Az alrendszer telepítésével kapcsolatos szakmai szempontok érvényesítését célozza a veszélyes üzemi monitorozási terv, amely alapján készülnek a kivitelezési tervek.

A monitorozási terv tartalmi elemei a következők:

- a veszélyes ipari üzemek és azok közvetlen környezetének bemutatása, a veszélyes létesítmények és az ott jelen levő veszélyes anyagok azonosítása;
- a hatásterületek (veszélyességi övezetek) kijelölése és a területvédelmi elv alkalmazásával a területek rangsorolása;
- a veszélyes anyagok terjedési tulajdonságainak meghatározása;
- a veszélyes anyag és meteorológiai monitoring üzemi és települési végpontjai telepítési helyeinek elhelyezkedése.

Az üzemi monitoring rendszer kialakításánál figyelembeveendő legfontosabb elvek az alábbiak:

- a monitoring rendszer katasztrófavédelmi feladatok megvalósítását szolgálja;
- a monitoring végpontok elhelyezésénél és az érzékelők jelzési és riasztási szintjeinek beállításánál legfontosabb szempont a lakosság védelme, azaz olyan értékeket kell meghatározni, amely védelmi tervek aktiválását és a

lakosságvédelmi intézkedések bevezetésének szükségességét vonja maga után;

- a monitoring végpontokat – a területvédelem elvének alkalmazásával – az üzem határainál úgy kell elhelyezni, hogy azok keresztezzék a lakóterületek irányába terjedő felhő útját.
- a veszélyes anyag kibocsátásának helyét és anyagmennyiségeket konzervatív megfontolások alapján a legkisebb felhőszélességgel járó eseményekre alapozni indokolt;
- a végpontok telepítési sűrűségénél figyelemmel kell lenni arra, hogy a két végpont között a mérgező gázfelhő lehetőleg ne haladjon el anélkül, hogy valamelyiket érintené;
- az éghető gázok monitorozásakor figyelembe kell venni azt, hogy a gázfelhő késői gyújtása robbanáshoz vezethet, ezért a monitoring végpontok telepítését a számított robbanási zónán kívülre kell tervezni;
- a védett településen lehetőség szerint két végpontot az érintett település üzemhez legközelebb található szélén kell telepíteni;
- a meteorológiai érzékelőkkel is ellátott végpontoknak a védelmi irányokban való elhelyezésekor a környezeti és a meteorológiai feltételek mellett figyelembe kell venni az üzemi épületek és építmények elhelyezkedését is;
- a gáz- és a meteorológiai érzékelők mérési tulajdonságainak megállapításakor figyelemmel kell lenni a projekt céljaira alkalmazott mérőműszerek mérési tulajdonságaira.

Jelzési és riasztási szintek meghatározása

A monitoring rendszer katasztrófavédelmi célokat szolgál, így a legfontosabb feladat a lakosság védelme. A projekt céljaira a legtöbb EU tagállamban és az USA-ban is alkalmazott az ERPG (Emergency Response Planning Guidelines) 2 és 3 érték került kiválasztásra. A levegővel robbanóelegyet képező szénhidrogén gázok koncentrációjának mérésénél a jelzési szint az ARH 40 %-a, riasztási szint, pedig az ARH 60%-a.

A monitoring alrendszer a belső és a külső védekezés szerves része

A több éves projekt keretében megvalósuló monitoring rendszer szervesen beépül az üzemi (belső) és a települési (külső) védelmi tervekbe, a vezetés és a lakosságvédelmi intézkedések bevezetésének folyamatába. A rendszer alapot szolgáltat a védelmi tervek kellő időben való életbeléptetéséhez, amely a súlyos baleset bekövetkezésekor jelentősen csökkentheti annak következményeit.

Kommunikációs és informatikai-adatátviteli rendszer

A MoLaRi rendszer alapvetően hierarchikus felépítésű és négy szintet különböztet meg:

- helyi szint
- települési szint
- megyei (vagy regionális) szint
- országos szint

Helyi szinten a veszélyes üzemeket, illetve azok környezetét értjük. Itt helyezkednek el a monitoring mérőhelyek végpontjai, valamint a lakossági riasztó rendszer végpontjai.

Alapvető követelmény a végpontokkal szemben az autonóm működés lehetőségének a megvalósítása.

Ez a vegyi monitoring és a meteorológiai monitoring végpontok szempontjából a következőket jelenti:

- hálózati tápfeszültség kimaradása esetén is meghatározott ideig működőképes maradjon,
- a kommunikáció megszakadása esetén a mért adatokat gyűjtse.

Lakossági riasztó végpont szempontjából a következőket jelenti:

- hálózati tápfeszültség kimaradása esetén is meghatározott ideig működőképes maradjon,
- alkalmas legyen helyi üzemmódban működni és riasztást kiadni.

A helyi szinten elhelyezett eszközök a területi adatgyűjtő központtal állnak kapcsolatban, ide küldik a mérési eredményeket (monitoring), valamint a műszaki állapotról, illetve a hozzáférésről (pl: ajtónyitás) szóló állapot jelentéseket. Ezeket az adatokat az egyes végpontok a rendszer paraméterezésekor meghatározott időközönként továbbítják, de bármilyen állapot változás esetén ez azonnali hatállyal megtörténik mind a műszaki állapotban történt változás esetén, mind a monitoring rendszerben bekövetkezett előre definiált határérték átlépése esetén. A területi adatgyűjtő központ irányából a végpontokhoz kérések (pl. állapot azonnali lekérdezése) és utasítások (pl. riasztás kiadása) is érkezhetnek, melyeket a végpont haladéktalanul végre hajt. A végpontokat a nagyfokú rendelkezésre állás érdekében redundáns adatátviteli kapcsolat köti össze a területi adatgyűjtő központtal.

A kialakítandó rendszernek települési szinten két eleme található meg:

- területi adatgyűjtő központ,
- Hívatósos Önkormányzati Tűzoltóságok ügyeleti terminálja.

A területi adatgyűjtő központ feladata:

- a monitoring és lakossági riasztó végpontokról származó mérési eredmények és állapot jelzések fogadása, tárolása és a megyei szint felé való továbbítása,
- a megyei szint felől érkező kérések (azonnali mérés, műszaki állapot) fogadása és továbbítása a végpontok felé,
- a megyei szint felől érkező utasítások (riasztás) továbbítása a végpontok felé.

A fenti feladatok maradéktalan ellátása érdekében a területi adatgyűjtő központ egységes rendszerelemekkel kerül kialakításra mind a monitoring, mind a lakossági riasztó végpontok irányába. A magas fokú rendelkezésre állás érdekében szünetmentes tápegységgel kerül kialakításra. Az adatok átmeneti tárolásához elegendő tárhelytelenséggel rendelkezik.

A területi adatgyűjtő központ és a megyei szintet redundáns átviteli kapcsolat köti össze. A Hívatásos Önkormányzati Tűzoltóságok ügyeleti termináljai a központi szinten elhelyezkedő adatbázishoz kapcsolódnak, saját adatbázissal nem rendelkeznek.

Az ügyeleti terminálok lehetővé teszik:

- a rendszerben tárolt információk megjelenítését,
- központi szintről érkező jelzések fogadását, nyugtázását,
- helyszínrajzok, térképek megjelenítését.

Az ügyeleti terminálok notebook kivitelben GPRS adatkapcsolattal kerülnek kialakításra, ami lehetővé teszi a települési ügyelet esetleges kiköltöztetése esetén is az események folyamatos nyomon követését. A megyei szinten helyezkednek el a rendszer megyei központjai és a Megyei Katasztrófavédelmi Igazgatóságok ügyeleti termináljai. A megyei szintet az országos szinttel redundáns adatátviteli kapcsolat köti össze. A Megyei Katasztrófavédelmi Igazgatóságok ügyeleti termináljain – jogosultságtól függően – a rendszer összes szolgáltatása elérhető. Az ügyeleti terminálok a kiszolgáló szerverekkel redundáns módon kerülnek összekötésre. Az országos szinten helyezkedik el a rendszer országos központja, az Országos Katasztrófavédelmi Főigazgatóság ügyeleti termináljai és a Műszaki Főügyeleti Központ termináljai. Az Országos Katasztrófavédelmi Főigazgatóság ügyeleti termináljai szolgálnak a monitoring rendszer adatainak a megtekintésére és a szükséges intézkedések végrehajtására. A Műszaki Főügyeleti Központ termináljai a rendszer állapot jelzéseinek fogadását és a hibaelhárítások irányában tett intézkedések végrehajtását és dokumentálását teszik lehetővé. Az ügyeleti terminálok a szerverekkel redundáns módon kerülnek összekötésre. A MoLaRi rendszert az angolszász szakterminológia szerint egy mission critical rendszernek tekintjük, ezért mind a szándékos támadással szembeni, mind, pedig a műszaki meghibásodásból eredő fenyegetettségnek rendkívül ellenállóvá kell tenni.

A rendszer bázisát képező szerverek, valamint aktív adatátviteli berendezések konstrukciója rendkívül robusztus és jelentős nemzetközi referenciákkal rendelkező szállítóktól, a Fujitsu-Siemens és a Cisco vállalatoktól származnak. Valamennyi aktív berendezés szabványos, 19"-os, zárható szekrényben kerül elhelyezésre, amely különleges kiképzése egyúttal biztosítja a berendezések szellőzését is. A központi szerverközpont tartalék energiaellátását puffer üzemben töltött akkumulátorok, leválasztó inverter és automatikusan induló dízel generátor biztosítja. A végpontok tartalék energiaellátása szünetmentes tápegységről történik. Az adatbázis és alkalmazás szerverek Windows 2003 operációs rendszer alatt üzemelnek. A Windows 2003 operációs rendszerre épülő cluster szoftver réteg lehetőséget ad robusztus szerver szoftverek üzemelésére mind terhelés megosztásos (load balancing), mind szolgáltatás átvételes (fail over) üzemmódban. Ezen üzemmódok, kihasználására kerül sor az adatbázis-kezelők és az alkalmazás szerverek működtetésekor. A helyi központokban Windows 2003 operációs rendszer üzemel, amely feladata a helyi adatgyűjtés, pontos idő továbbítása a végpontok felé, az üzemi diszpécserközpontok részére ellenőrző jelleggel a mért adatok megjelenítése, valamint naplózás. A helyi központokban két számítógép elhelyezésére kerül sor, amelyek együttműködése biztosítja a szükséges redundanciát. Az ügyeleti terminálok operációs rendszere Windows XP Pro. Erre egyfelől a grafikus megjelenítés, másfelől a chip-kártyás autentikáció miatt van szükség.

A legfelső szinten elhelyezkedő szerverközpont, a regionális kommunikációs központok és a helyi központok közötti adatátvitelt egy 100%-an tartalékolt IP hálózat valósítja meg. Az IP hálózat elsődleges útvonalai optikai szál valamint mikrohullámú technológia segítségével kerülnek megvalósításra. A tartalék útvonal kiépítése mikrohullámú vagy ISDN technológia alkalmazásával történik. A teljes rendszer adatsomag szintű forgalmazását dinamikus útvonal kiválasztó rendszer (routing internet protocol - RIPv2) vezérli. A helyi központok és az érzékelő, valamint sziréna végpontok közötti adatátvitel ipari szabványokon alapul, hordozója csomag szinten az IP protokoll és tartalékoltan kerül kiépítésre. A szerverközpontban, valamint a helyi központokban a helyi hálózat tartalékoltan kerül kiépítésre. Így két LAN kapcsoló egyidejű üzemeltetésére kerül sor. A MoLaRi rendszer érzékelőinek mérési adatait, valamint az érzékelők és szirénák állapot adatait a helyi központtól a szerverközpont veszi át és tárolja az adatbázis-kezelőben. Az adatbázis-kezelő terhelés megosztásos (load balancing), két-számítógépes üzemmódban üzemel. Így az adatbázis-kezelés szintjén az egy hibából származó üzemkiesés (single point of failure) kiküszöbölésre kerül. A monitorozó és riasztó alkalmazás a szerverközpontban üzemel. Az alkalmazást funkció átvételes (fail over) két-számítógépes rendszer működteti.

A rendszer kliens-szerver architektúrájú, amely vezérli a működést, tárolja és feldolgozza az adatokat, biztosítja az adatok lekérdezését az igényeknek megfelelően. Biztosítja a központi letölthetőséget és a verzió kontrollt. Az ún. vékony klienses megoldást alkalmazzuk, mely esetében a klienseken egy böngésző fut, a kliens oldal ennek használatával valósul meg. Az alkalmazás biztosítja - az arra jogosult felhasználók számára - a hozzáférést, a jogosulatlan hozzáférést egyértelműen kizárja és naplózza, biztosítja a felhasználóhoz és művelethez kötött naplózás lehetőségét.

Lakossági riasztó és tájékoztató rendszer

Az elmúlt évek üzemeltetési tapasztalatai alapján a MoLaRi rendszerben egyértelmű megoldásként az elektronikus riasztó és tájékoztató eszközök alkalmazása kerül előtérbe. A riasztó rendszer adatgyűjtő és vezérlő átviteli útját duplikáltan, nagy biztonságú hálózatokon, a rendszerek üzemvitelét biztosító energia ellátást alapvetően az országos villamos energia hálózat igénybevételel tervezzük megvalósítani. A rendszerek állapotának figyelése és a riasztás végrehajtása valós idejű és folyamatos üzemvitelű lesz. A végpontok és a helyi szintű központi vezérlő állomás közötti kommunikációt a MOTOROLA CANOPY vezeték nélküli szélessávú IP átviteli rendszerrel, majd a 2007 végétől az országos lefedettséget elérő EGYSEGES DIGITÁLIS RÁDIÓTÁVKÖZLŐ (EDR) rendszer felhasználásával kívánjuk biztosítani. A rendszer funkcionalitása megköveteli, hogy a központi vezérlő állomás közvetlen kapcsolatban legyen az összes, a körzetébe tartozó végponttal. Ezen azt kell érteni, hogy csoportkommunikáció formájában kell tudnia elérni az összes érintett végpontot, pl. egy aktiválás elrendelése alkalmával. E funkciót biztosítja redundáns módon az EDR és a Canopy rendszerek együttműködése. A vezérlő állomás maximum 200 végpontot tud kiszolgálni. Ez, a számok ismeretében, miszerint átlag kb. 40 sziréna végpont jut egy helyi szintű központra, bőven elegendő. A végpontok kiépítése során fontos követelmény, hogy kiegészítő, támogató szolgáltatások a rendszerbe kritikus átalakítások nélkül integrálhatók legyenek („kisbíró” üzemmód, WEB kamera telepítése, szöveges tájékoztatás).

A rendszer kiépítését a 21 üzem által veszélyeztetett települések érintett területein kívánjuk telepíteni, melyek mennyiségét az alábbi táblázat tartalmazza:

Veszélyeztetett település		Szükséges szirénák (db)
Algyő	2008	9
Budapest	2008-12	393
Dorog	2010	6
Dunaújváros	2009	27
Gógánfa, Ukk	2007	4
Kazincbarcika, Berente	2006	9
Oszlár	2006	2
Peremarton gyártelep, Berhida, Papkeszi	2007	4
Pétfürdő, Várpalota, Ősi (2 üzem)	2007	23
Pincehely	2008	4
Sajóbábony	2006	4
Sajószentpéter	2006	6
Tiszapalkonya	2006	3
Tiszaújváros (Szabadidő Központ, Erőmű lakótelep)	2006	7
Újudvar	2011	4
Százhalombatta, Ercsi	2007	60
Összesen:	2006-2012	565

A rendszer megvalósításának első ütemében Borsod- Abaúj –Zemplén megyében lévő 5 kiemelt veszélyes ipari üzem által érintett településeken összesen 31 lakossági riasztó és tájékoztató végpont kerül telepítésre (lásd: táblázat vastagított része). A riasztás elrendelését biztosító vezérlőközpontok az illetékes megyei (fővárosi) igazgatóságok ügyeletein kerülnek telepítésre, a végpontok szabad csoportképzéssel lesznek indíthatók. A riasztó rendszer kiépítési konstrukciója lehetővé teszi a rendszer bővíthetőségét, a már telepített elektronikus eszközök beintegrálását az újonnan kiépítendő rendszerbe. Egy riasztó végpont az alábbi főbb egységekből épül fel:

- elektronikus sziréna hangsugárzó(k),
- energia ellátó blokk (erősáramú hálózat becsatlakozás, tartalék áramforrás).
- szirénavezérlő egység,
- redundáns adatátviteli interfészek.

Az akusztikus tájékoztató és riasztó rendszerek esetén az egyik legfontosabb tényező a folyamatos üzemkésztség biztosítása. Ennek megvalósításához általában olyan eszközre van szükség, mely a felsorolt paramétereket folyamato-

san képes ellenőrizni (mérni), és normálistól eltérés esetén jelentést küld egy központi helyre. Az eszköz kiválasztása folyamán gondos mérlegelés eredményeképpen a Motorola által gyártott MOSCAD rendszerre esett a választás. A MOSCAD ipari célokra kifejlesztett távfelügyeleti, vezérlő és adatgyűjtő rendszer. Fejlesztésénél fő szempont volt a vezetékek nélküli adatátvitel sajátosságainak figyelembe vétele. A MoLaRi rendszer lakossági riasztó és tájékoztató alrendszerének alapvető feladata -a monitoring alrendszer vegyi anyag specifikus mérőszondái által generált riasztási jelzések alapján a veszélyes ipari üzem veszélyeztetettségi övezetében lévő települések polgármesterei részére a külső védelmi tervekben megfogalmazott lakosságvédelmi feladatok közül – a lakosság azonnali riasztása és tájékoztatása a bekövetkezett eseményekről. A rendszer kiépítését bővíthetően kívánjuk megvalósítani, hogy biztosítani tudjuk más monitoring rendszerek jeleinek fogadását, illetve újabb üzemek esetén azok bekapcsolását. A mért adatok hozzáférhetőségét WEB-es felületen keresztül az OKF Főügyeletén, az üzemek által érintett Megyei Katasztrófavédelmi Igazgatóságok ügyeletén az érintett Hivatásos Önkormányzati Tűzoltóságok ügyeletén biztosítjuk. A megvalósuló rendszert korszerű, nagybiztonságú informatikai berendezésekkel, már meglévő és üzemelő átviteli csatornákon (kormányzati gerinc, BM adathálózat, BM mikrohullámú gerinc) és üzemelő (később megvalósuló) redundáns hálózatokon (GPRS, EDR) kívánjuk működtetni.

Dr. Ványa László:

Út a szoftverrádiók és szoftver rádiózavaró állomások felé

Bevezetés

A szoftverrádió, más kifejezéssel a szoftver vezérlésű rádió (SDR - Software Defined Radio) az utóbbi tíz évben rohamosan fejlődésnek indult területe az infokommunikációs technológiáknak. Szinte már közhelynek számít, hogy az ezredfordulóra az informatikai eszközök és a hírközlés robbanásszerű fejlődése, majd integrációja leváltotta az analóg hírközlő rendszereket és beköszöntött a digitális korszak. Mára világossá vált, hogy a vezetékes és vezeték nélküli digitális hírközlő eszközök nem jelentették a fejlődés csúcsát, mert a lényeg nem a jelek digitalizálásában rejlik, hanem abban, hogy a digitalizálással olyan eljárásokra, tervezési és konstrukciós megvalósításokra nyílt lehetőség, amelyek addig elképzelhetetlenek voltak.

Jelen előadás azt az utat követi végig, amelyet a kommunikációs eszközök és a zavarásukra szolgáló elektronikai hadviselési berendezések bejártak a kezdetektől a digitális korszak beköszöntéig, majd arra a kérdésre keresi a választ, hogy milyen irányban haladva lehet a legkorszerűbb szoftverrádiók által jelentett kihívásokra megtalálni az elektronikus zavarás válaszait.

Az analóg hírközlés kora

A 20. század hajnalán megjelentek az első már távközlésre alkalmas rádió berendezések és igen gyorsan alkalmazásba vették mind a polgári, kereskedelmi rádiózásban, mind a hadseregekben. Az első berendezések szikratávírók voltak, amelyek méretüknél és energia-felvételüknél fogva elsősorban stabil szárazföldi, vagy hajófedélzeti alkalmazásokra voltak alkalmasak. Háborús viszonyok között az 1904-1905-ös orosz-japán háborúban alkalmazták őket először, ahol a felek mind a saját, mind az ellenséges adásokat észlelték. Felismerve ennek felderítési, hírszerzési jelentőségét, megkezdődött a rádiólehallgatás, a rádióbemérés, a közlemények akadályozása rádiózavarok alkalmazásával, majd hamarosan megjelentek a megtévesztő, dezinformációs célú rádióadások és a közlemények lehallgatását akadályozó rejtjelzési eljárások is. Elkezdődött a rádióháború, mai szóhasználatunkkal az elektronikai hadviselés.

A hírközlésre és az ellene folytatott felderítő, zavaró tevékenységre szolgáló berendezések műszaki fejlődése párhuzamosan folyt. Az első 50-60 év során ennek az volt a közvetlen oka, hogy a lehallgatási és zavarási feladatokat ugyanazokkal az adó-vevő berendezésekkel hajtották végre, amelyeket a híradásra használtak, esetleg egy-két kiegészítő egységgel látták el őket, mint például a zavarmodulátorok, vagy a vizuális analizátorok. Az elektroncsöves technológia fejlődése lehetővé tette a viszonylag kisméretű, akár telepes táplálású, mobil eszközök kifejlesztését, ami oda vezetett, hogy minden repülőgép,

harcjármű és kisalegység rendelkezett az ötvenes évekre saját rádióberendezéssel.

A háborús tapasztalatok hatására és a hidegháborús modernizációs folyamatban tudományosan elméletben is megalapozták az elektronikai eszközökkel vívott harc módszertanát, majd létrehozták a világ több országában azokat a speciális eszközökkel ellátott alegységeket, amelyek alapfeladata a rádiófelderítés, lehallgatás, és zavarás lett. Megjelentek a rádióspektrum vizuális megjelenítésére szolgáló berendezések, a panoráma analizátorok, amelyek lehetővé tették a kezelők számára, hogy egyidőben széles frekvenciatartományt tekinthessenek át, észlelhessék a megjelenő kisugárzó eszközöket, ráhangolhassanak, majd a közlemények rögzítésén túl méréseket végezzenek az elfogott rádióadás paraméterein.

Az analízis során a kezelők kiképzettsége, begyakorlottsága volt a meghatározó az adásmódok azonosításában, a minél gyorsabb paraméter meghatározásban, és nem utolsósorban a nyelvtudás szintje játszott fő szerepet a közlemények tartalmának rögzítésében. A különböző manuális és gépesített rejtjelző eszközök munkaigényes alkalmazásával viszonylag rövid ideig sikerült csak a közlemények fedését biztosítani, mivel a kulcsok váltása és más technikai problémák nehezítették az alkalmazók dolgát. A másik oldalon már a második világháború éveire komoly erővé nőtte ki magát a kriptóanalízis, amire példaként elég az Enigma rendszerrel folytatott küzdelmet említenünk.

Az alkalmazott adásmódok tekintetében viszonylag kisszámú eljárást alkalmaztak, azok is inkább csak egy-egy fő adásmód modifikációi voltak. A berendezés konstrukciókra az volt a jellemző, hogy az úgynevezett „áramkörkapcsolt technikát” alkalmazták, vagyis minden egyes adásmódhoz a hozzá tervezett áramköröket, egységeket kapcsolták az alapegységeknek tekinthető fokozatokhoz. Ilyen alapegység például egy vevőkészülék esetében például az antenna, az antenna előerősítő, a helyi oszcillátor, a középfrekvenciás erősítő, vagy akár a hangfrekvenciás végfokozat. Az adásmódtól – modulációs módtól – függően azonban különböző keverőfokozatokra, demodulátorokra, szűrőegységekre volt szükség, amelyeket kapcsolók segítségével váltogathattak a feladatnak megfelelően. Az adókban hasonlóképpen választottak modulátorokat, szűrőket és más szükséges fokozatokat.

Egy-egy ilyen berendezés a gyártásból kikerülve élettartama végéig ugyanazt tudta, változtatásra, továbbfejlesztésre nem volt mód. Ennek köszönhetően egy újabb adásmód megjelenésekor az akár kiváló műszaki állapotban lévő eszközöket is csak teljesen cserélni lehetett. A berendezés építés egy adott szintjén megjelentek a moduláris egységek, az oldható csatlakozókkal való szerelések, így esetleg arra nyílt lehetőség, hogy ha a gyártó kifejlesztette az adott berendezéshez szükséges új áramköröket, akkor mintegy technikai támogatásként a piacra dobva azokat, az alkalmazó utólag egységcserével korszerűsíthette a berendezését a teljes csere helyett.

Az analóg korszak második része a félvezetős elektronika forradalma idejére tehető. Erre a korra az volt a jellemző, hogy a berendezések méret és energia-felvételének csökkentése céljából az elektroncsövekhez képest megbízhatóbb és hosszabb élettartamú tranzisztoros áramkörökkel váltották ki a korábbiakat, ahol csak erre lehetőség volt. Egyes területeken, mint például a nagyfeszültségű, nagyfrekvenciás és a nagyteljesítményű elektronikában ez az átállás lassabban haladt, sőt még ma is vannak olyan áramköri alkalmazások, amelyekből nem sikerült az elektroncsöveket kiszorítaniuk a félvezetőknek. Megjelentek a hibrid konstrukciók, a részben tranzisztoros, részben csöves berendezések, illetve a teljesen tranzisztorizált készülékek is. Felépítésükre továbbra is jellemző maradt a modularitás, de elsősorban a gyors javíthatóság miatt, a továbbfejlesztések esetén továbbra is csak a készülékek cseréje volt a megoldás.

Az adásmódok tekintetében tapasztalható fejlesztéseket nem igazán az elektroncső-tranzisztor generációváltás gerjesztette, hanem például az olyan kutatások gyakorlati alkalmazásba vétele, mint a kiterjesztett spektrumú adásmódok különböző válfajai. A '80-as évekre az integrált félvezetőtechnológiára épülő számítástechnika és a megfelelő eszközök birtokában feltörekvő vezérléstechnika, méréstechnika és híradástechnika egy jelentős, bár kérészerűtlen fejlődési lépcsőt hozott létre. Az egyre inkább előregedő csöves, és a különálló egységekből álló tranzisztoros berendezéseket az új gondolat szellemében olyan berendezésekkel kell leváltani, amelyek egymással kommunikálni képesek, parancsokat és adatokat fogadhatnak, továbbíthatnak, adott algoritmusoknak megfelelő teljes folyamatokat hajthatnak végre.

Megszülettek a berendezéseket a külvilággal összekapcsoló szabványos interfészek, a kommunikációs nyelvek, programok (pl. a CP/M nyelv, a HP-IB busz szabvány, az RS-232, RS-432 stb.) és az eddig különálló berendezések összekapcsolhatóvá váltak. Óriási fejlődés volt ez, mert a digitális vezérléstechnika pl. olyan komplex mérőrendszerek megépítését tette lehetővé, amely mérési folyamatok távolról való végrehajtását, technológiai folyamatok automatizált irányítását, kontrollálását tette lehetővé. A buszrendszer utasítások és adatok kétirányú forgalmával biztosította az egységek együttműködését. Az ilyen rendszerekben tehát kezelőszervekkel és távvezérlő jelekkel is működtethető „műszerek” üzemeltek, szabványos interfészekkel csatlakoztak egymáshoz, így lehetővé vált egy irányító eszköz, például egy vezérlőprogram futtató számítógép irányításával a komplex feladat szervezett végrehajtása.

A továbbfejlesztéshez, vagy egy új feladat végrehajtásához új vezérlőprogramot kellett írni, azt letölteni a rendszervezérlő számítógépbe és már indulhatott is az új feladat. Minőségileg új, pl. szélesebb frekvenciatartományban való működést biztosító továbbfejlesztés esetén az alapkészülékeket kellett kicserélni és a program szükséges módosításait elvégezni. A '80-as, '90-es

évek technikai modernizációs hullámában ily módon elgondolt automatizált mérő-ellenőrző rendszerek épültek, számítógép vezérelte automatizált rádiózávaró berendezések és más vezetési eszközök készültek el többek között a Magyar Honvédség elektronikai hadviselési csapatai számára, de más országokban is.

Ezek a rendszerek új működési algoritmusokkal működtek, egyre több feladatot láttak el emberi beavatkozás nélkül, ugyanakkor konzerválták az analóg adástechnikát, és a környezet megváltozása után, a digitális adásmódok megjelenésekor nem is voltak képesek az újat követni. Minden analóg rádióadás-, vétel- és méréstechnikai eszközt egyidőben kellett volna kicserélni, de az az időközben elavult vezérlő számítógépek teljes leváltását is megkövetelte volna.

Ezzel az analóg korszak a végéhez ért, vagyis ezek a berendezések semmiféle fejlesztéssel, javítással sem műszakilag, sem gazdaságossági szempontból nem lettek volna alkalmasak a további használatra, ezért teljes generációváltásnak kellett, (kellett volna) következni.

A digitális korszak első időszaka

A kilencvenes évekre kifejlesztésre kerültek és nagy számban alkalmazásba kerültek azok a modern kis valószínűséggel felderíthető, digitális adásmódokat alkalmazó polgári és katonai hírközlő rendszerek, amelyek a kor színvonalán a modern integrált gyártástechnológiával már gazdaságosan, nagy mennyiségben előállíthatók voltak. A korábbi évtizedektől eltérően nem a katonai kutatás-fejlesztés eredményei kerültek a polgári alkalmazásokba át, hanem az egyre nagyobb magántőke bevonásának köszönhetően a polgári fejlesztések eredményei kerültek katonai alkalmazásokba. Ez többek között a két világrendszer szembenállásának megszűnésével, a katonai kiadások, többek között a fejlesztési kiadások drasztikus lecsökkenésével is magyarázható.

Olyan korábban katonai területeken szereztek fölényt a polgári alkalmazások, mint az űrtávközlés, az űrtávérzékelés, de a földi vezetékes és vezeték nélküli távközlési hálózatok is dominánsan a polgári fejlesztési színvonal mentén haladtak. A katonai hírközlési és elektronikai hadviselési rendszerek harcában úgy tűnt, hogy a hírközlés jelentős lépéselőnyre tett szert. Az elavult EH rendszerek már alkalmatlanok voltak akár csak a digitális berendezések jeleinek érzékelésére is, nemhogy a paramétereik megmérésére, vagy a szükséges és hatékony zavaró jelek előállítására.

Néhány más forrásból ismert és szabványos üzemi adatokkal üzemelő rendszer lefogása a hagyományos eszközökkel, főleg zajzavarokkal lehetővé vált, de ezekben az eljárásokban sokkal inkább a nyers erő érvényesült, mint az intelligens módon előállított optimális zavarójel tervszerű hatása. Ily módon lefogható pl. a GPS műholdas navigációs rendszer, ugyanakkor egy harctéri rádió lefogása napjainkban komoly problémát jelent.

A költségvetési megvonások a világ valamennyi országában fékeztek az új követelményeknek, kihívásoknak megfelelni képes elektronikai hadviselési berendezések kifejlesztését, ugyanakkor még a legnagyobb költségvetésből fejlesztő amerikai hadsereg is belefutott az automatizált, korszerű térinformatikai eszközöket használó, de az analóg rendszert konzerváló fejlesztés zsákutcájába, amint azt a Ground Based Common Sensor[1] projekt mutatta is. A projektet az elért sikerek ellenére a fentebb vázolt okok miatt le kellett állítani és a Prophet[2] elnevezésű fejlesztési programban, teljes irányváltás után teljesen újra kellett kezdeni.

Mindeközben a távközlési eszközök és a számítástechnikai rendszerek tovább fejlődtek. A korszakra jellemző az a digitális adástechnika, amely egyrészt már kibővített frekvenciatartományban több együttműködő számára vált elérhetővé, a hanginformáción kívül szöveges üzenetek, adatállományok cseréjére is alkalmas lett és hálózatokba volt kapcsolható, beépített, elsősorban hardveres titkosító algoritmusokkal biztosította a megfelelő védeltséget a lehallgatás, megfajtás ellen. Ezek a készülékek elsősorban a haderőnemek közötti interoperabilitást célozták meg, bár a korszakra jellemző módon a többnemzetiségű béketeremtő, békefenntartó műveletekben az együttműködő nemzetek csapatai számára továbbra is komoly problémákat okoztak az eltérő üzemmódok, titkosítási eljárások és más műszaki problémák amelyeken gyorsan úrrá kellett lenni a szövetséges hadműveletek sikere érdekében.

Ebben az időben a mikroelektronika olyan nagyteljesítményű proceszorokat kezdett előállítani, olyan nagy műveleti sebességű jelfeldolgozó áramköröket (DSP – Digital Signal Processor) és speciálisan egy adott feladatra kifejlesztett áramköröket (ASIC – Application Specific Integrated Circuit) gyártott, amely technikailag elért egy olyan küszöböt, amely egy újabb technikatörténeti minőségi ugrást tett lehetővé. Ez az ugrás nem volt más, mint az úgynevezett szoftverrádiók megalkotásának a lehetősége. Ez az alig tízéves múltira visszatekintő terület már most sokkal több forradalminak nevezhető hatást hozott, mint előtte sok tíz év.

A szoftverrádió

A szoftver vezérlésű rádió, rövidebb elnevezésével a szoftverrádió a Software-Defined Radio (SDR) Forum [3] definíciója szerint: „olyan rádiótechnológia, amelyek szoftveres úton lehetővé teszi a modulációs eljárások széles körének kiválasztását, a széles, vagy keskenysávú üzemmódokat, a forgalmazás különböző eljárásokkal való rejtését, titkosítását, az adott hullámsávban jelenleg, vagy akár a jövőben használatos szabványok, eljárások rugalmas beépítését, alkalmazását. A szoftverrádió technológia a olyan funkcionális moduloknak szoftveres eszközökkel egy rádiórendszerbe való összekapcsolása, mint pl.:

- az oszcillátor (jelgenerátor);

- modulátor/demodulátor;
- kódoló (kapcsolati réteg protokollok);
- sokszorozók/osztók, stb.;”

Az SDR technológia lehetővé teszi a programozható hardver modulok összekapcsolását és ennek a nyílt architektúrának a felhasználó igényeinek leginkább megfelelő szoftverrel való együttműködtetését. A rádiókészülékek alapvető paramétereit meghatározó oszcillátorok, modulátorok, demodulátorok, kódolók, dekódolók, titkosítók és az együttműködést meghatározó kapcsolati réteg protokollok működését és jellemzőit a szoftver határozza meg, így szükség esetén az egész rendszer egy szoftver frissítéssel újabb szabványok alkalmazására tehető alkalmassá, vagy akár egy újabb berendezés típusú alakítható át. Ezáltal az egész berendezés, vagy csak akár a hardverelemek cseréje nélkül, modernizálhatók ezen eszközök. Ez jelentős gazdasági megtakarítást is jelenthet, és azt is, hogy egy adott gyártmányt csupán szoftvercserével alkalmassá lehet tenni egy egészen eltérő működési környezetben való alkalmazásra. Ily módon lehetővé válik az is, hogy ugyanazon típusú berendezést több ország a saját nemzeti titkosító algoritmusaival üzemeltessen.

Kissé leegyszerűsítve a szoftverrádió technológia azt jelenti, hogy csak szoftver kérdése, hogy ugyanaz a berendezés Bluetooth, WLAN, GPS, Radar, WCDMA, GPRS, vagy más berendezésként üzemel.

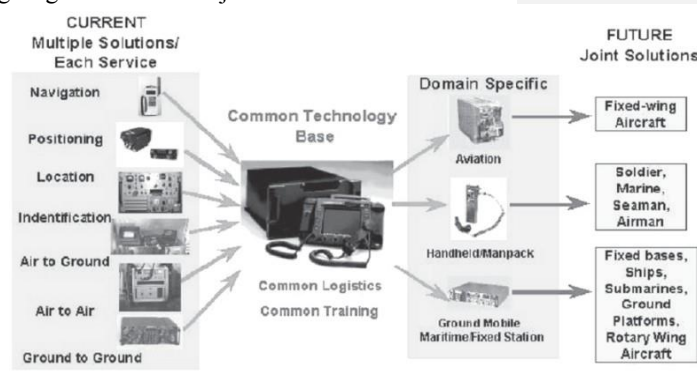
A technológia kidolgozása céljából alakult meg mintegy 50 hírközlésben érdekelt cég együttműködésével a Modular Multifunction Information Transfer System Forum on Software Defined Radio nevű szervezet a '90-es évek közepén.

Az első katonai szoftverrádió program az Egyesült Államokban SPEAKeasy[4] néven indult 1992-ben. A program első fázisának az volt a célja, hogy olyan rádiót dolgozzon ki, amely a 2 MHz – 2 GHz frekvenciasávban lehetővé teszi a szárazföldi erők, a légierő, a haditengerészet és a műholdas rádiórendszerek együttműködését. A projekt eredményeit teljes sikerrel demonstrálták a 21. Századi Haderő digitális dandár gyakorlatán 1997-ben. A vevőkészülék antennából, erősítőből, keverőből, erősítésszabályozó áramkörökből és analóg-digitál konverterből állt, amelyeket VME bus rendszer kapcsolt össze egy sor Texas C40 DSP-vel. Az adó digitál-analóg konverterből, egy frekvenciakonverterből (up converter - keverőből), teljesítményerősítőből és antennából állt, amelyet PCI busz kötött össze. Az igen széles működési frekvenciatartományt több analóg rádiófrekvenciás alsávi egységre bontással biztosították, amelyet ugyanahhoz az analóg-digitál konverterhez kapcsoltak.

A SPEAKeasy program második szakaszában olyan gyorsabban átkonfigurálható rendszer kidolgozását tűzték ki célul, amely nyitott szoftver architektúrán képes különböző rádiós protokollok között bridge-ként működni, a korábbiaknál kisebb, könnyebb és nem utolsósorban olcsóbb is. Az eredetileg három évre tervezett programot tizenöt hónap után leállították és az elké-

szült 4-400 MHz között működő rádió gyártásba került. Ebben a programban alkalmaztak első ízben FPGA-kat (Field Programmable Gate Array – programozható kapusor áramkör).

Az USA és a NATO szövetségesek a Joint Tactical Radio System (JTRS)[5] programban együttműködve fejlesztettek szoftverrádiót. A cél egy rugalmas, interoperábilis rendszer kidolgozása volt, amely egy szoftveres kommunikációs architektúrára építve, a CORBA és POSIX operációs rendszerek segítségével harmonizálják a különböző szoftver modulok működését.



1. sz. kép. A JTRS rendszer[5]

A szoftverrádiók működését az adott rádióra jellemzően az ún. hullámforma (waveform) határozza meg, amely a felhasználói bemenettől a rádiófrekvenciás kimenetig, a vett jel feldolgozási módjától a felhasználónál megjelenő információig mindent beállít. Ennek a magyar katonai szakirodalomban való első részletesebb feldolgozását Hóka Miklós doktori értekezése (illetve annak részpublikációi) tárgyalja.[6]

Ma az SDR Forum nevű nemzetközi szervezet az, amelyik célul tűzte ki az üzleti célú, nyílt platformú szoftverrádiók kutatását, fejlesztését, a kapcsolódó szabványok kidolgozását, javaslatok nemzetközi rádiós fórumok elé vitelét.

A szoftver rádiózavaró rendszerek fejlesztésének perspektívái

A fentiek alapján megállapíthatjuk, hogy a szoftverrádiók fejlődése igen gyors ütemben halad, szinte naponta születnek újabb és újabb alkalmazások például a wireless hálózatok és a mobil rádiórendszerek továbbfejlesztésében. Már a ma meglévő „építőkövek” és eljárások képességei, teljesítménye lehetővé tenné, hogy azokból a hagyományos rádiófelderítés feladatainak minden tekintetben megfelelő vevőkészülékek, analízátorok legyenek kifejleszthetők. A megfigyelt spektrumtartományokban vett jelek analízisét, kategorizálását és

azonosítását FFT eljárással lehet megoldani, a DSP-k segítségével kinyert adatok eltárolhatók a zavarás tervezéséhez.

A zavaró adók semmiben nem különböznek a „hagyományos” értelemben felépített adó berendezésektől, illetve csak annyiban, hogy az adott céljelre való optimális zavar előállítását egy számítógépes program végzi és állítja be. Az ilyen filozófiájú és rugalmasan konfigurálható, széles frekvenciasávban működő elektronikai zavaró berendezések mind a hagyományos katonai hírközlő eszközök, mind a polgári rendszerek elleni feladatok végrehajtására is alkalmasak lehetnek.

Véleményem szerint egy teljesen a szoftverrádió filozófiára épülő új elektronikai hadviselési eszközrendszer kifejlesztésének ma műszaki-technikai akadályai nincsenek, hanem döntés és feladatszabás, valamint nem kevés anyagi erőforrás kérdése. Ehhez persze a mai, korszerű körülményekre illeszkedően meg kell határozni a végrehajtandó feladat mennyiségi és minőségi paramétereit, azokhoz a szükséges berendezések harcászati-műszaki követelményeit, majd a végrehajtandó folyamatokat, eljárásokat. Ezután meg kell határozni a hordozó szükségletet, majd a rendszer vezetéséhez és üzemeltetéséhez szükséges szervezeti kereteket kidolgozni. Ez nem kevés munka, de az elektronikai hadviselés mai színvonalán nincs más megoldás, mert most olyan időket élünk, amikor nem szabad régi, elavult berendezések összevásárlásával látszatképeket létrehozni.

FELHASZNÁLT IRODALOM

- [1] Ground-Based Common Sensor (GBCS Heavy and Light)
<http://www.fas.org/irp/program/collect/gbcs.htm>
- [2] Prophet <http://www.fas.org/irp/program/collect/prophet.htm>
- [3] SDR Forum honlapja www.sdrforum.org
- [4] Software-defined radio http://en.wikipedia.org/wiki/Software-defined_radio
- [5] Joint Tactical Radio System Programmable, Modular Communications System <http://www.globalsecurity.org/military/systems/ground/jtrs.htm>

Dr. Vass Sándor alezredes:

Az infokommunikációs berendezések elektronikai védelmének néhány aktuális kérdése

Bevezetés

A XXI. századi életünk minden területét behálózzák már az elektronikus információt gyűjtő, tároló, feldolgozó és továbbító infokommunikációs eszközök.

A korszerű hadseregekben is tömegesen alkalmaznak olyan infokommunikációs eszközöket, amelyek létfontosságúak a felderítő rendszerekben, a csapatok vezetésében és a fegyverek irányításában. Az elektronikai hadviselés jelentőségét egyre növeli az a tény, hogy az intenzív felkészülésen kívül egyes elemeit (az elektronikai felderítést, illetve az ellene való védelmet és a nem szándékos elektromágneses zavarok elkerülését célzó tevékenységeket) a szemben álló felek már békében is aktívan folytatják.

Elektronikusan tárolt adataink védelme is veszélybe kerülhet, ha nem készülünk fel az információs rendszereink logikai védelme mellett azok elektronikai védelmére. Míg az elektronikus térben (pl. számítógépes hálózatok) az információ biztonság kiforrott eszközökkel rendelkezik, addig a fizikai térbe kerülő információ védelme nincs kielégítően megoldva. Ugyanakkor fel kell készülnünk arra, hogy az infokommunikációs eszközeink megfelelő védelemmel rendelkezzenek az újabb, illetve eddig kevésbé ismert (elektromágneses pusztító) támadó eszközökkel szemben.

Az érzékeny elektronikai berendezések, infokommunikációs rendszerek üzemeltetésénél nem szabad figyelmen kívül hagyni a természetes zavarforrásokat sem, tehát például a villámcsapások hatásaival is számolnunk kell. Ezért szükséges az infokommunikációs berendezéseink elektronikai védelmének és tökéletesítési lehetőségeinek vizsgálatára.

1. Elektronikai védelem területei

A rendkívül sok és nagy mennyiségű elektronikai eszköz és különösen képpen az infokommunikációs berendezések széleskörű alkalmazása fokozottabb kihatással van az új harcmódok és harcelfjárások kialakítására. Az elektronikai védelem a korszerű fegyveres küzdelemben meghatározó fontos tényezővé, a fegyverek és csapatok hatékonyságát jelentősen befolyásoló erővé vált.

Az elektronikai védelem az elektronikai hadviselés azon része, amely biztosítja az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére.

Az elektronikai védelem alapvetően három fő területre osztható fel, úgymint:

- az elektronikai felderítés elleni tevékenység;
- az elektronikai ellentevékenység elleni tevékenység; és
- az elektronikai ellenőrzés. [1]

A felderítés elleni tevékenység magába foglalja az elektromágneses kisugárzások korlátozását és a felderítés előli kitérés különböző módozatait. Az elektronikai ellentevékenység elleni tevékenységhez a szándékos és a nem szándékos elektromágneses zavarok elleni tevékenységek továbbá elektronikai pusztítás elleni védelem tartozik. Az elektronikai ellenőrzés pedig az előzőekben említett két fő terület rendszabályai betartásának ellenőrzését foglalja magába. Ugyanakkor az elektronikai védelem sikeres megvalósítása megköveteli a szoros együttműködést az elektronikai hadviselés más összetevőivel is.

2. Az elektronikai felderítés elleni védelem

A felderítés elleni tevékenység célja észlelni, megbecsülni és megakadályozni az ellenséges felderítési adatok gyűjtését, továbbítását, feldolgozását és szétosztását. A felderítő eszközök elleni védelem feladatait mind békében, mind háborúban folyamatosan és maradéktalanul végre kell hajtani.

Az infokommunikációs eszközökről és rendszerekről azok üzem közbeni kisugárzása során, valamint funkcionális feladataikból adódó áruoló jelek alapján szerezhetők be információk. Tehát a felderítés elleni tevékenység alapvető tartalma ezen áruoló jellemzők kiküszöbölése vagy minimálisra csökkentése.

Az elektronikai felderítés elleni tevékenységnek az elektromágneses spektrum teljes szélességére ki kell terjednie, melynek megvalósítása számos módszer és tevékenységet eredményez, ezek közül emelek ki néhányat.

2.1. A nem szándékos elektromágneses kisugárzás felderítés elleni védelme

Az infokommunikációs rendszereken belül a számítógépes hardverek elektromágneses kisugárzása (lehallgathatósága) már az 1960-as években felmerült. Az amerikai NSA (*National Security Authority*) az 1970-es években TEMPEST (*Transient ElectroMagnetic Pulse Emanations Standard*) néven programot indított a probléma vizsgálatára; amely a keretét adta a későbbi, az elektromágneses lehallgatás ellen védett készülékek tervezésére, és gyártására vonatkozó TEMPEST szabványoknak.

A nem szándékos kisugárzás elleni védelem olyan intézkedések és eszközök alkalmazását jelenti, amelyek célja az áthaladó információ illetéktelen megjelenítésének és az elektromos berendezések kompromittáló kisugárzása analizálásának megakadályozása. Az átviteli utak és végberendezések által keltett kisugárzások illetéktelen detektálása és rögzítése azért veszélyes, mert nem érzékelhető az információk kompromittálódása vagy olyan rendszerinformációk megszerzése, amely további támadásokhoz szolgálhat támpontként.

A védelmi rendszabályok irányulhatnak eszközökre és működési környezetre. [2]

Működése során minden elektronikus eszköz létrehoz olyan elektronikus erőteret, amelynek érzékelésével a működésre vagy a kezelt (továbbított) adatokra vonatkozó információk szerezhetők be, akár illetéktelen személyek által is. Ennek megelőzése érdekében az eszközöket olyan aktív és passzív védelmi elemekkel kell kiegészíteni, amelyek ezeket a nem szándékosan kisugárzott jeleket árnyékolják, vagy más módon semlegesítik. Védendő eszközök alatt nemcsak a végberendezéseket kell érteni, hanem ide kell sorolni az összes olyan eszközt (kapcsolók, szerverek stb.), amelyek az összetett átviteli út során biztosítják az adatok továbbítását.

A helyiségek kompromittáló kisugárzás elleni védelmének lényeges területe a helyiségekből kivezető csövek (víz, gáz, fűtés) megfelelő szigetelése - beleértve a hanghullámok tovaterjedésének vizsgálatát és a megakadályozását is -, a vezetékek (erős- és gyengeáramú kábelek) szűrése és a megfelelő földelési rendszer kialakítása. Azokat a helyiségeket, ahol nagy mennyiségű számítástechnikai eszköz van elhelyezve egy, ún. Faraday-hálóval, azaz a helyiség mind a hat falába beépített földelt fémhálóval szokták védeni. Elektromágneses kisugárzás ellen védeni kell a LAN-ok hálózatát is. Ehhez árnyékolt kábeleket célszerű használni. Előfordulhat, hogy az elektronikus eszközökből a táphálózatra jutnak ki jelek, amelyek a tápáramra szuperponálódnak. Ezeket megfelelő eszközökkel a támadó távolabbról is kiszűrheti, ezért az elektromos hálózat szűrésére, leválasztására is szükség van.

2.2. Rádiófelderítés elleni védelem

A rádióálcázás a rádió felderítés elleni védelem leghatékonyabb eszköze, amely különböző szervezési és technikai rendszabályokkal biztosítható.

A rádióálcázás rendszabályai a következők lehetnek:

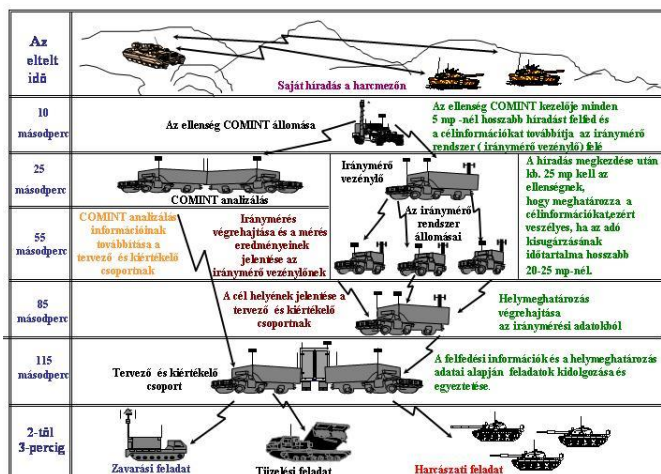
- a helyzettől függően a rádióállomások adásának teljes vagy részleges betiltása (rádiótilalom);
- az információ legrövidebb idejű átfutását biztosító rádióforgalmi rendszer és üzemmód megváltoztatása;
- az adóállomások kisugárzásának korlátozása csak az információtovábbítás idejére;
- a korábbi forgalmi adatok felhasználásának megtiltása átcsoportosításkor és áttelepüléskor;
- a rádióállomások minimálisan szükséges teljesítménnyel való üzemeltetése, irányított antennák, illetve az összekötetés létesítéséhez szükséges legoptimálisabb antennák alkalmazása;
- a rádióállomás kezelők munkájára jellemző sajátosságok megszüntetése stb. [3]

Az előbb felsorolt rendszabályok közül az *elektromágneses kisugárzás korlátozása* (Emission Control- EMCON) a siker kulcsa lehet az ellenséges hatásokkal szemben, amelyek felfedik, megakadályozzák, zavarják a saját infokommunikációs rendszereink üzemét. Az adóberendezéseket csak a feladat végrehajtásához szükséges időtartalmig szabad bekapcsolni, mivel az ellenség felderíti, analizálja rendszereinket és megkeresi azokat a kisugárzókat, amelyekből használható információt nyerhet.

Amikor kisugárzási tilalom van - vagyis a rádióadóink nincsenek bekapcsolva - az ellenség felderítése nem tudja felfedni elektronikai rendszereinket. Ebben az esetben a kisugárzás korlátozása teljes. Akkor is érvényesül a kisugárzás korlátozása, amikor a parancsnok elhatározása alapján rádió tilalmat vagy rádiócsendet vezetnek be.

Az adó berendezéseket csak minimális ideig szabad bekapcsolni (az ajánlott kisugárzási idő 15 másodperc, amely nem haladhatja meg a maximális 20 másodpercet), amely idő alatt az információt is továbbítani kell.

Ez a módszer azonban egyedül nem képes kiküszöbölni a saját adóink felfedését és iránymérését, ezért kombinálni kell más felderítés elleni módszerekkel is, amelyek tovább nehezítik adóink települési helyének meghatározását. Az 1. sz. ábrán felderítés és célmegjelölési folyamat időtartalma látható. Az ábrán látszik, hogy a folyamat viszonylag rövid időt vesz igénybe. E rövid idejű tevékenység ellen hatásos lehet az elektronikai eszközeink kisugárzásának csökkentése, amellyel megakadályozhatjuk, hogy a szemben álló fél felfedje, analizálja és hatást gyakoroljon saját elektronikai rendszereinkre.



1. sz. ábra. A szemben álló fél felfedés és iránymérés folyamata [4]

3. Elektronikai ellentevékenység elleni védelem

Az elektronikai ellentevékenység elleni védelmen belül alapvetően az infokommunikációs eszközök szándékos és nem szándékos zavarok elleni védelmével foglalkozunk részletesen.

Az egyes infokommunikációs eszközök zavarvédeltségét alapvetően a fejlesztés-, tervezés-, kivitelezés során kell biztosítani, és lehetővé tenni, hogy a berendezések minél nagyobb mértékben legyenek képesek kiszűrni a zavarokat.

3.1. Az elektromágneses zavarok kialakulásának körülményei

Az infokommunikációs eszközöket vizsgálva az elektromágneses zavarást előidéző jel alapvetően két forrásból fakadhat:

- Magából a vizsgálat alá vett eszközből, rendszerből. Ebben az esetben belső eredetű zavarról beszélünk.
- Eszközön, rendszeren kívülről. Ez más berendezés (rendszer) által generált elektromágneses tér által okozott külső eredetű zavar lehet.

Vezetett zavar az, amely fémes vezetők közvetítésével galvanikusan, kapacitív vagy induktív csatoláson keresztül terjed:

- *galvanikus csatolás*, ahol a zavaró hatások az áramkörök közös (ohmos) elemein keresztül jönnek létre. A zavaró jellemző az áram;
- *kapacitív csatolás*, ahol a zavaró hatások a váltakozó villamos terek útján kerülnek a zavaró áramkörből a berendezés zavart részébe. A zavaró jellemző a feszültség;
- *induktív csatolás*, ahol a zavaró hatások egy zavarforrás váltakozó mágneses tere által indukált feszültségként keletkeznek a zavart elszennvedő vevőben. Okuk a zavarforrás áramának változása. [1]

A vezetett zavart előidéző jelek elsősorban a berendezések tápellátását biztosító kábeleken vagy a földvezetéken keresztül zavarják meg más áramkörök működését.

Sugárzott zavarás, ahol a zavart olyan szabadon terjedő elektromágneses hullámok okozzák, amelyek becsatolódnak a berendezés egyes részeibe. A befolyásoló tényező a szabadon terjedő hullámok esetén az elektromos és a mágneses tér, vezetéken terjedő hullámoknál a vezetésbeli áram és feszültség.

Sugárzott zavarásról beszélünk abban az esetben, ha a zavarójelet valamilyen közegen keresztül (pl. légkör) az elektromágneses tér terjedése közvetíti.

Az előzőekben leírtak alapján megállapítható, hogy valamely infokommunikációs eszköz, rendszer zavarviszony vizsgálatának ki kell terjednie mind a vezetett és sugárzott emisszióra, mind pedig a vezetett és sugárzott elektromágneses zavarokkal szembeni érzékenységre (a rendszer tűrőképességének vizsgálatára).

3.2. Zavarás kialakulásának folyamata

Az elektromágneses zavar és mértéke három tényező függvénye, úgy-
mint:

- a zavarforrás paraméterei, elsősorban a spektrumsűrűség;
- a zavart közvetítő közeg, vagy vezetési tulajdonságokkal rendelkező anyag átviteli karakterisztikája;
- a zavart elszennvedő berendezés, áramkör, alkatrész érzékenysége. [1]

Az elektromágneses zavarás kialakulásának folyamatát bemutató 2. sz. ábra bár egyszerűnek tűnik, a valóságban - éppen a három tényező sokfélesége miatt - bonyolult folyamatot takar. A bonyolultságot az okozza, hogy a valós közvetítő közegben telepített rendszereket az esetek döntő többségében előre meg nem határozható zavarforrások veszik körül, miközben a rendszerek elemei is létrehozhatnak belső eredetű zavarokat.



2. sz. ábra. Az elektromágneses zavarás kialakulásának folyamata

Minden üzemelő, elektromágneses energiát kisugárzó adóállomás - a hullámterjedés sajátosságait figyelembe véve - kelt valamekkora elektromágneses térerősséget az üzemelő vevőállomások bemenetén.

Egy, a zavart elszennvedő - adott feltételek között működő - vevőállomás zavarásának mértéke erősen függ:

- a zavarforrás frekvenciájától, üzemelési időpontjától, területi elhelyezkedésétől;
- mindkét berendezés modulációs módjától;
- a hasznos jel és a zavarforrás által keltett jel térerősségének arányától;
- a zavart elszennvedő vevőállomás és a zavarforrás antennájának iránykarakterisztikájától;
- a hasznos jel és a zavarforrás által keltett jel polarizációjának eltérésétől;
- a zavart elszennvedő vevőállomás frekvenciafüggő átviteli és demodulációs jellemzőitől stb.

A zavarforrás zavart okozhat, ha:

- a zavarforrásból származó energia a zavart elszennvedő vevő számára a hasznos jelnél - a zavarállóságot is figyelembe véve - nagyobb;
- a zavarforrásból származó energia frekvenciaspektruma egybeesik a zavart elszennvedő vevő vételi sávjával.

3.3. A rádiózavarok elleni védelem lehetőségei

A rádiózavarok lehetnek:

- szándékos, a kommunikáció megbénítása céljából létrehozott zavarok;
- kölcsönös, a többi üzemelő kommunikációs és más rádiótechnikai eszközök által okozott zavarok;
- légköri (atmoszférikus), a különböző természeti jelenségek által keletkezett zavarok;
- helyi elektromos, a helyi áramforrások és más berendezések által keltett zavarok. [3]

Általános zavarvédelmi elv, hogy első lépésként megpróbáljuk csökkenteni a zavarforrás kibocsátását. Ha ez nem megy, akkor megkísérelhetjük csökkenteni a zavarjellel terhelt infokommunikációs berendezésünk zavarérzékenységét. Ezek után egyetlen lehetőségünk van: a zavarjel-adó és a zavart elszennvedő berendezés közötti csatolást (amelyen keresztül a rádiófrekvenciás zavaró jelek eljutnak a rendszerünkbe) kell úgy alakítani, hogy jelentősen csökkentse a zavarjel energiáját.

A csatolás csökkentésekor általában mindkét bejutási módra gondolnunk kell: a legtöbb esetben a sugárzott és vezetett zavarok nagyságát ugyancsak csökkenteni kell. A csökkentés mértékére jellemző csillapítást általában dB-ben szokás megadni, számítása:

$$a = 20 \log S1/S2$$

ahol: az a = a csillapítás értéke [dB];

az $S1$ = a csatolás előtti jelszint;

az $S2$ = a csatolás utáni jelszint (ez kerül a zavart elszennvedő berendezésre). [5]

3. 3. 1. A szándékos zavarok elleni védelem módszerei, eszközei

A szándékos zavarok hatásuk jellege szerint lehetnek:

- célzott, félcélzott és elfogó;
- modulált, manipulált, impulzus- és kombinált zavarok. [3]

A szándékos zavarás hatékonyságát csökkentő általános módszerek a következők lehetnek:

- a zavarás és zavarok felismerése:
 - a zavar eredetének meghatározása (a zavar külső, ha a zavar az antennán keresztül jut be a vevőbe, a zavar belső, ha a zavar nem az antennán keresztül jut be a vevőbe [berendezés hiba]);
 - a zavar hovatartozásának meghatározása (a zavar szándékos, pl. ellenséges zavarás esetén; a zavar nem szándékos, pl. saját eszköz zavarása, atmoszféra zavarok stb. estén).
- a zavarás és a zavarok hatékonyságának csökkentése:
 - az üzemelés folytatása (a zavar hatékonyság felmérésének akadályozása céljából);
 - a hasznos jel és a zavaró jel arányának javítása;
 - a vevőberendezés be szabályozása (helyi oszcillátor, sáv szélesség, hangerő stb. be szabályozása);
 - az adó kimenő teljesítményének növelése;
 - az antenna be szabályozása vagy megváltoztatása (antenna polarizáció megváltoztatása minden állomáson, nagyobb terjedelmű antenna alkalmazása);
 - átjátszó állomás létesítése;
 - az antenna helyének a megváltoztatása;
 - alternatív híradó útvonalak alkalmazása;
 - frekvencia megváltoztatása;
 - másik műholdra való átállás.

Az információs rendszerekben és az azokat támogató infrastruktúrákban széleskörűen alkalmaznak kommunikációs berendezéseket. Ezért fel kell készülni ezen eszközök zavarás elleni védelmére.

A rádióhíradás zavarok elleni védelme (zavarvédetség fokozása) szervezési és technikai rendszabályokkal biztosítható.

A zavarvédelem fontosabb szervezési intézkedései a következők lehetnek:

- tartalék frekvenciák kijelölése;
- az ellenség által is alkalmazott frekvenciasávok (frekvenciák) felhasználása a saját rádióhíradásban;
- a rádiótávíratok, közlemények több frekvencián történő leadása, illetve több vevővel történő vétele;
- a rádióállomások üzem módjának helyes megválasztása;
- rejtett rádióforgalmi rendszerek szervezése;
- helyettesítő (dublirozó) rádióforgalmi rendszerek szervezése;

- a rádióhíradás kerülőirányainak felhasználása;
- közbeeső rádióállomások alkalmazása;
- zavarvédett rádióeszközök, vagy speciális berendezések alkalmazása;
- az üzemi és tartalék frekvenciák közötti eltérés kellő megválasztása. [3]

A fentiek közül mindig azon módszert célszerű alkalmazni, amely a legnagyobb zavarvédeettséget biztosítja a zavarás ellen.

A zavarvédelem fontosabb technikai intézkedései a következők lehetnek:

- irányított antennák és speciális antennarendszerek alkalmazása;
- az adóteljesítményének növelése;
- a vevő áteresztési sávjának megváltoztatása;
- a vett rádiójel kellő hangszínének beállítása;
- a vett közlemények rögzítése (pl.: magnetofonnal történő vétele) többszöri vétel biztosítása céljából;
- a terep kedvező sajátosságainak (pl. árnyékoló hatásának) kihasználása a rádióállomás telepítésekor. [3]

Az adók teljesítményének növelése ugyan az ellenség szándékos zavarása elleni védelem legegyszerűbb módja, de ez a saját nem szándékos zavarok jelentős növekedéséhez vezethet. Egyben megkönnyíthetjük az ellenség rádiófelderítését, így fokozhatjuk berendezéseink megsemmisítésének valószínűségét. Ezért a teljesítménynövelést akkor célszerű alkalmazni, amikor már kimerítettük a szándékos zavarok elleni védelem összes többi lehetőségét.

A térszelekció az élesen irányított adó- és vevőantennák alkalmazásával biztosítható, amelynek megvalósítása az ultrarövid-hullámú sávban már nem ütközik nehézségbe. Az antenna sugárzási diagramjának forgatásával, fázis-kompenzációs módszerrel a zavaró jelek elnyomhatók. Nézzük meg közelebbről e technikai módszer lényegét.

A vevőberendezésnél egymástól néhány üzemi hullámhossz távolságra két vevőantennát telepítünk merőleges iránnyal a hasznos jel sugárzási irányára. A kisugárzott hasznos jeleket két antennával egyidejűleg vesszük, azaz egyenlő fázissal. Ha a hasznos jel frekvenciáján zavarás van, és ha a zavaró jel kisugárzási iránya különbözik a hasznos jel kisugárzási iránytól, akkor a vevőantennák a zavaró jelet bizonyos fáziskülönbséggel veszik.

A zavaró jel elnyomásához meg kell változtatni a hasznos és zavarójel közötti fáziskülönbséget (mivel a két antenna között fellépő fáziskülönbség 180 fok), majd pedig amplitúdóit is egyenlővé kell tenni. A fáziskülönbség megváltoztatását fázisfordítóval, az amplitúdók kiegyenlítését pedig az antennákra épített variométerrel és szintautomatikával lehet végrehajtani.

A két ellentétes fázisú és különböző amplitúdójú jel összegzésének eredményeként a vevő bemenetén a hasznos jel a zavarójelhez képest kisebb gyengülést szenved. Időszелеkció alkalmazása esetén a vevőberendezések csak a hasznos jel megjelenésének időszakában működnek.

Amplitúdó- szelekció a vevőfokozatban a különböző zajvágó áramkörökkel hozható létre. Frekvenciaszelekció a vevőberendezésben alkalmazott különböző rezgőköri elemekkel érhető el. (Viszonylagos egyszerűségénél fogva ez a legjobban elterjedt szelektivitást növelő módszer.)

A szándékos zavarok elleni védelem fokozásának további módszere a védett kódok alkalmazása. Azokat a kódokat nevezzük vételzavar védetteknek, amelyekkel az üzem során a kódokat rejtjel-kombinációban felfedjük, bizonyos feltételek mellett pedig ki is javítjuk a hibákat.

A fent megvizsgált szándékos zavarok elleni védelmet fokozó módszerek csak a zavarok egy bizonyos csoportjára hatásosak. Ugyanakkor napjainkban az elektronikai eszközök zavarvédeltségét fokozó technikai módszerek egyetlen ismert eszköze sem biztosítja az elektronikai zavarás elleni teljes védeltséget. A zavarvédeltség megoldását a szervezési és technikai módszerek komplex alkalmazásában kell keresni.

Korszerű viszonyok között az elektronikai hadviselésen belül a saját elektronikai rendszereink, eszközeink szándékos zavarok elleni védelmének új területei látnak napvilágot, ezek a területek még igen sok megoldatlan szervezési és technikai problémát vetnek fel.

A szándékos zavarok elleni védelem általános módszereinek áttekintése után megállapítható, hogy azokat egyrészt szervezési (pl. alternatív híradó útvonalak), másrészt technikai (pl. az adó kimenő teljesítményének növelése) módszerekkel lehet biztosítani.

3. 3. 1. Az elektromágneses impulzus eszközök elleni védelem módszerei és eszközei

Napjainkban bárki „kis műszaki érzékkel” könnyen előállíthat kisméretű, hatékony elektromágneses pusztító eszközöket, amelyek valós veszélyt jelenthetnek az infokommunikációs berendezéseink üzemeltetésére. Ezért az érzékeny elektronikai berendezéseinket védenünk kell az elektromágneses impulzusoktól a szervezési rendszabályok szigorú betartásával, illetve különböző technikai eszközök és módszerek alkalmazásával.

Könnyű kijelenteni, hogy meg tudjuk védeni az infokommunikációs eszközeinket az elektromágneses impulzusokkal szemben, de megvalósítani nem olyan egyszerű. Az elektromágneses impulzusok elleni védelem alapvető problémája, hogy nem ismert az elektromágneses impulzus nagysága a védett eszköznél. Így nehéz megállapítani, hogy milyen nagyságú elektromágneses

impulzust kell lecsökkenteni olyan mértékre, amelyet még károsodás nélkül elviselnek az érzékeny elektronikai eszközök. A szükséges érték ismeretében lehetőség lenne meghatározni azt az optimálisan szükséges védelmi módszert és eszközt, így nem kellene minden esetben a maximális védelmi értéket biztosító eljárást vagy eszközt alkalmazni.

Az elektromágneses impulzusok elleni védelem eszközei lehetnek:

- árnyékoló és elnyelő anyagok;
- szikraközös villámhárító eszközök;
- hálózati szűrők;
- fémoxid varistorok;
- elektrooptikai eszközök;
- nagy sebességű zener diódák. [6]

Az árnyékoló és elnyelő anyagokkal az elektronikai eszközök teljes lefedésével ideális védelem biztosítható az elektromágneses impulzusok ellen, bár ilyen védelem megvalósítása az esetek többségében nem lehetséges, mivel más elektronikai berendezésekkel is biztosítani kell a kapcsolatot. A leghatékonyabb ilyen védekezés az úgynevezett „Faraday kalitka”. Ez egy fémből, vagy fémhálóból készült doboz, amelybe belehelyezve az adott elektronikai eszközt, az védve van a külső elektromágneses tér elől.[7]

A szikraközök alaptípusának felépítése és működése egyszerű. Két elektróda között szigetelőréteggént levegő helyezkedik el. Alaphelyzetben az elektródák között a szigetelőréteg miatt nem folyhat áram, ezért ez az állapot a kapcsoló nyitott helyzetének felel meg. Ha az elektródák közötti feszültséget emeljük, akkor elérjük azt a feszültséget, amelyen bekövetkezik az átütés, és elektromos ív alakul ki. Az ív nagyon kis ellenállású elektromos összekötésnek tekinthető, ezért ez az állapot a kapcsoló zárt helyzetének felel meg. Az átütési feszültséget az elektródák távolsága határozza meg: úgy állítják be, hogy az átütés hamarabb következzen be a szikraközben, mint a védett fogyasztóban. [8]

A hálózati szűrők alkalmazásával kiszűrhetők az elektromos és számítógépes adathálózaton terjedő zajok, zavarok és túlfeszültségek, amelyek a tápegységek, adatátviteli eszközök korai meghibásodásához vezethetnek. [9]

Az adatátviteli vonalakon a túlfeszültség tovaterjedése elleni védelemre sikeresen alkalmazható dióda, varisztor, gázlevezető, melyeket érdemes kombinálni. A dióda az egyenfeszültséget nem engedi át a berendezés felé, míg a gázlevezető túlfeszültség esetén hirtelen leföldeli a rendszert.

Elektrooptikai eszközök alkalmazásával megoldható az adatátviteli kábelek védelme. Ezen eszközök széleskörűen alkalmazhatók az adat és kommunikáció

kációs csatornáknál, az energiafigyelő és irányító rendszereknél, az ellenőrző irányító rendszereknél, az őrzésvédelmi rendszereknél és egyéb biztonsági rendszereknél. [10]

A nagy sebességű zener diódák működése azon alapszik, hogy belső ellenállását igen gyorsan megváltoztatja (rövidre zár) ha a rákötött feszültség hirtelen megnövekszik, illetve átlépi a meghatározott küszöbszintet. A korszerű zener diódáknál a folyamat sebessége a 10^{-9} másodperc, az elméleti határ pedig 10^{-12} másodperc is elérheti. Eltérően a varistoroktól a zener dióda jellemzői többszöri túlterhelés hatására sem változnak.

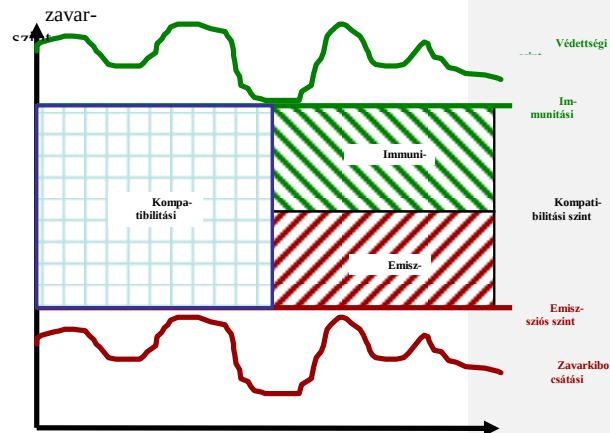
3. 3. 2. Az infokommunikációs rendszerek nem szándékos zavarok elleni védelmének módszerei, eszközei

Minden villamos működésű készülék és berendezés vagy elektronikus rendszer, -mint például az infokommunikációs rendszer is - a környezetével állandó elektromágneses kölcsönhatásban van. Egyrészt a saját környezetükre elektromágneses hatást fejtenek ki, így esetenként megengedhetetlenül nagy elektromágneses zavarok forrásai is lehetnek, vagy fordítva, a környezetükben fellépő elektromágneses hatások az érzékeny berendezések működésében különböző zavarokat, hibás működést is előidézhetnek, vagy esetenként a berendezés meghibásodását vagy teljes tönkremenetelét is okozhatják.

Valamely eszköz elektromosan kompatibilisnek tekinthető egy adott környezetben, ha a környezete által keltett elektromágneses tér jelenlétében megfelelően tud működni, illetve működése közben az általa keltett elektromágneses tér a környezetét nem zavarja. Ezért kell arra törekedni, hogy az elektronikai eszközök közötti elektromágneses kompatibilitás folyamatosan biztosítható legyen.

A zavarok elkerülhetők, ha meghatározunk egy olyan zavarkibocsátási küszöböt minden villamos eszközre, rendszerre, amelyet ha nem lép túl, nem okoz problémát a környezetében. Ugyanakkor minden villamos eszközre, rendszerre meg kell állapítani egy zavarérzékenységi küszöböt, azt a határértéket, amely alatti zavar szinteknél még üzembiztosan, helyesen működik a berendezés. Ha ezt a két küszöbszintet egymáshoz illeszkedően, helyesen választjuk meg, a villamos berendezéseink kompatibilisek, vagyis zavartalanul fognak üzemelni.

Minden készülék egyben gerjesztője, egyben elviselője az elektromágneses zavarkörnyezetnek. A 3. sz. ábra alapján akkor kompatibilis az elektronikus készülék elektromágneses szempontból a környezetével, ha az általa kibocsátott zavar megfelelően kicsi és az immunitása nagy.



3. sz. ábra. Zavarkibocsátási és zavarérzékenységi szintek meghatározása [11]

Az infokommunikációs eszközök közötti elektromágneses kompatibilitást:

- a tervezés;
- a gyártás;
- az üzemeltetés előtti rendszertervezés;
- az üzemeltetés

időszakaiban kell biztosítani.[1]

A korszerű elektromágneses kompatibilitás-tervezéseknél ma már egyre inkább a „rendszer szemléletű” tervezési módszert alkalmazzák, amelyet számítógépes analízáló programokkal oldanak meg. A programok interaktív jellegűek, s figyelembe veszik a zavarforrásokat, a közvetítő közegek lehetséges változatait és a zavart elszenvedő rendszer, alrendszer, berendezés érzékenységét.

A tervezés során figyelembe veszik a már üzemelő berendezésekkel szerzett tapasztalatokat és a várható alkalmazási terület szabta speciális követelményeket is.

Az infokommunikációs eszközök gyártása során szigorúan be kell tartani a szabványokat, technológiai utasításokat, a beépített alkatrészek üzembiztonságára és paramétereire vonatkozó követelményeket, és az elkészült berendezéseket ellenőrizni kell az elektromágneses kompatibilitás szempontjából.

Az infokommunikációs eszközök gyártását követően az üzembe helyezés előtt meg kell vizsgálni, hogy az adott paraméterekkel rendelkező elektronikai eszköz (rendszer) zavarmentesen üzemeltethető-e a tervezett alkalmazási körzetben, illetve okoz-e zavarást a környezetében üzemelő elektronika eszkö-

zöknek. Abban az esetben, ha az adott elektromágneses környezetben az új infokommunikációs eszköz (rendszer) üzemeltetésével elektromágneses zavarás alakulhat ki, szervezési rendszabályokkal (teljesítmény, terület, időkorlátozásokkal) kell biztosítani az infokommunikációs eszközök (rendszerek) zavarmentes üzemeltetését.

Az elkészült, és az elektromágneses kompatibilitásra vonatkozó szabványoknak megfelelő infokommunikációs berendezések üzemeltetésekor szigorúan be kell tartani a kezelési utasításokban előírt rendszabályokat valamint a megadott szinten kell tartani és rendszeresen ellenőrizni kell az elektromágneses kompatibilitással kapcsolatos paramétereket.

A rádió-berendezések közötti kölcsönös zavar kialakulása biztosítható:

- a rádióállomások pontos kalibrálásával, a rádióforgalmi rendszerek állomásainak pontos összehangolásával;
- ahol ez lehetséges, a keskenysávú üzemmód alkalmazásával;
- a rádióeszközök szabályos telepítésével;
- a térbeli széttelepítésre vonatkozó előírások betartásával, a terep domborzatának kihasználásával;
- az antenntípusok helyes megválasztásával a felületi, és térhullámú összeköttetések biztosítása céljából;
- a kölcsönös zavarok okainak feltárásával és megszüntetésével. [3]

3. 3. 3. Elektromos zavarok (túlfeszültségek) elleni védelem lehetőségei

A XXI. századi korszerű szolgáltatási szféra sem képzelhető el számítástechnikai eszközök és az ezeket összekapcsoló hálózatok nélkül.

A fenti rendszerek működésének feltétele a garantáltan folyamatos és zavarmentes villamos energia ellátás, azaz az ezeket működtető nagy- és kisfeszültségű ellátó rendszerek, hálózatok kifogástalan rendelkezésre állása.

Az infokommunikációs berendezésekben korábban alkalmazott integrált áramköröket viszonylag nagy villamos szilárdság jellemezte. A chipen belül az egyes alkatrészek egymástól mért távolsága időközben mintegy tizedére csökkent, és így ezek igen érzékennyé váltak a túlfeszültségekre. Ennek az a következménye, hogy ma már az adatátviteli vezetékeken viszonylag alacsony, néhányszor tíz voltos túlfeszültségek is elegendőek ahhoz, hogy pl. egy hálózatra csatlakozó PC hálózati kárttyáját tönkretégyék.

A legnagyobb hálózati túlfeszültségeket a villámkisülések okozzák. A külső villámhárító berendezést vagy a kiefeszültségű szabadvezeték közvetlenül érő villámcsapás esetén, - a nagy energiájú villám okozta túlfeszültségek miatt - sokszor átmenetileg ellátás nélkül maradnak hálózatra csatlakozó fogyasztók. A rendkívüli feszültség igénybevétele miatt a rendszer szigetelése is károsodhat.

A kapcsolási túlfeszültségek általában az üzemi feszültség két-háromszorosát érik el, míg a villámcsapás okozta túlfeszültségek értéke olykor a névleges feszültség húszszorosát is elérheti, ráadásul ezek mindig lényegesen nagyobb energiátartalmúak. Az üzemből való kiesés sokszor csak egy későbbi időpontban következik be, mivel az alkatrészek kisebb energiájú tranziensek általi többlet igénybevétele lappangva, szinte észrevétlenül károsítja az adott készülék elektronikájának elemeit.

A túlfeszültséget fokozatosan kell az adott helyen már veszélytelen értékre csökkenteni. Ésszerűnek és hatásosnak bizonyul az a villámvédelmi zóna-konceptió, amelyet az IEC 61312-1 nemzetközi szabvány ír le. Az elmélet lényege az, hogy a túlfeszültséget fokozatosan, még azt megelőzően csökkentjük egy veszélytelen szintre, mielőtt az a védendő készüléket elérné és abban kárt okozhatna. Az épület teljes energiahálózatát villámvédelmi zónákra (LPZ= *Lightning Protection Zone*) osztjuk. A különböző zónák találkozásánál lévő határfelületeket átlépő vezetékeken, - az adott besorolási osztály szintjének megfelelő megszólalási szintű - túlfeszültség-levezetőket helyezünk el. [12]

A rádióhíradás helyi elektromos zavarok elleni védelme elérhető:

- a rádióközpontok és önálló rádióállomások vevőberendezéseinek helyi elektromos zavarforrásoktól megfelelő távolságra való telepítésével;
- árnyékolt (koaxiális) antenna-bevezetők alkalmazásával;
- a zavarforrások megfelelő zavarszűrésével és árnyékolásával;
- a vevőkészülékeknek jó minőségű földelés elkészítésével;
- a rádióvevő-állomások, (központok) és az adatátviteli, távíró- és távbeszélő-állomások közötti távvezérlő, összekötő vezetékek szabályos építésével. [3]

Összegzés

Az elektronikai védelem azáltal, hogy csökkenti az ellenség felderítő és elektronikai ellentevékenységi lehetőségeit, minimálisra csökkenti a saját infokommunikációs kisugárzó eszközök által keltett nem szándékos zavarokat, jelentősen hozzájárul a saját csapatok élőerejének és technikai eszközeinek megővéséhez, és így nagy hatással van a saját harctevékenység sikerére.

Villamos hálózatokkal átszőtt világunk a növekvő információátvitellel együtt a zavarokra és a működéséhez szükséges adatátviteli, illetve távközlési hálózatok meghibásodásaira, üzemkieséseire igen érzékeny. Hosszabb ideig tartó meghibásodásuk akár katasztrófhelyzetet is előidézhet, ezért szükséges az elektronikai védelem szervezési és technikai rendszabályainak szigorú betartásával is biztosítani az infokommunikációs eszközök zavartalan és folyamatos működését.

Felhasznált irodalom

- [1] Dr. Vass Sándor – Dr. Balajti István: Elektronikai védelem, Budapest, ZMNE, 2000, J-1435.
- [2] Kassai Károly Az elektronikus információk védelmének területei <http://www.zmka.hu/kulso/mhht/hadtudomany/2002/3/kassaikaroly/chapter1.htm>
- [3] Magyar Honvédség Rádióforgalmi Szakutasítás, Hír/3, MH, Budapest, 2004
- [4] FM 24-33 Communications techniques: electronic counter-countermeasures <http://www.fas.org/irp/doddir/army/fm24-33/24330004.gif>
- [5] Mi is az az elektromágneses zavarvédelem? A túlfeszültség. <http://www.vgf.hu/villany/index.php?action=viewfull&ID=244>
- [6] Electromagnetic Pulse (EMP) And Tempest Protection For Facilities http://www.parallaxresearch.com/dataclips/pub/infosec/emsec_tempest/emp/emp.htm
- [7] Elemental Faraday Cage http://www.boltlightningprotection.com/Elemental_Faraday_Cage.htm
- [8] EMC villámvédelem és túlfeszültség-védelem V. rész: <http://epa.oszk.hu/00000/00025/00001/feher.html>
- [9] Eric Steven Raymond: Szünetmentes tápegység HOGYAN, <http://tldp.fsf.hu/HOWTO/UPS-HOWTO-hu/index.html>
- [10] Electromagnetic Pulse (EMP) And Tempest Protection For Facilities http://www.parallaxresearch.com/dataclips/pub/infosec/emsec_tempest/emp/emp.htm

- [11] Elektromágneses zavarvédelem 1. EMC fogalma, EMC szimuláció, csatlási formák.
http://www.ett.bme.hu/~nemeth/Elektr.%20kesz%20min/EMC_1.doc
- [12] Adatátviteli hálózatok védelme: <http://www.dehn.hu/>

Vörös Béla nyá. ezredes, okl. villamosmérnök:

Egyetemünk 1956-ban

Ebben az évben van az 1956-os forradalom és szabadságharc 50. évfordulója.

Akit érdekelt és napjainkban is érdekel a téma azt egyetemünk (Zrínyi Miklós Nemzetvédelmi Egyetem) kielégíti. Már az elmúlt évben megkezdődött a felkészülés és a publikálás. Az idei évben is ünnepségek, értekezések, kiállítások és hosszabb, rövidebb publikációk. emlékeznek meg erről az 50 évvel ezelőtti eseményről, melyben egyetemünknek jelentős szerep jutott. Pozitív és negatív történések láttak napvilágot, attól függően, hogy melyik rendszer értékeléseit olvassuk.

1956-ban két felsőfokú és három középfokú katonai tanintézet vett részt a harcokban.

A Zrínyi Miklós Katonai Akadémia, és a Petőfi Sándor Katonai Politikai Akadémia. Tiszti iskolák közül az összevont budapesti Kossuth Lajos tüzér és a Gábor Áron tüzér technikus Tiszti Iskola, a Szentendrén helyet kapott Zalka Máté híradó és Táncsics Mihály műszaki Tiszti Iskola. Bevetésre került még a Tatai laktanyában összevont Dózsa György lövész, páncélos és gépkocsizó Tiszti Iskola. Némely anyagban két iskola még a régi nevén szerepel, így a Petőfi akadémia Sztálin akadémia néven, a páncélos tiszti iskola Rákosi Mátyás néven.

Bár napjainkban már csak egy tisztképző intézmény létezik, az irodalomban a kornak megfelelően célszerű szétválasztva tárgyalni.

Az eddig megjelent írások egy-egy részt már a mai felfogásnak megfelelően tárgyalnak a korabeli eseményekről. Főként olyan írások látnak napvilágot az egyetem egykori állományából, melyek résztvevői az előző korban negatív beállításban szerepelnek. Ezek közül néhányat megemlítek.

Elsőnek talán az akadémia 1956-os parancsnokának visszaemlékezését : *Ezredesként a forradalomban* című Sári Katalin írását említem, az egykori híradó tanszékvezetőnek, Dr. Kolozsvári Sándornak írásait először az Új Honvédségi Szemlében olvashattuk. Urbán Vilmosnak *a Haza szolgálatában* című könyve is foglalkozik 1956-al. Király Béla szerkesztésében megjelent *Eltiprásuk és győzelmük 1956* című könyvében foglalkozik olyan eseményekkel, melyek érintik az akadémiát. Az elmúlt évben jelent meg az egyetem kiadásában a Társadalom és Honvédelem különkiadásában az *1956-os különszám*. Az egyetem Dr. Harai Dénes ezredes vezetésével készül fel a nevezetes évforduló ünnepi

programjának összeállítására. 2005-ben - halála előtt – az egyetem jelentette meg Haász János írását: *Tettem valamit a hazámért* című könyvét.

Az akadémia bekapcsolódik az eseményekbe

Az akadémián október 24-én hajnalban rendelték el ariadót. Minden katonai szervezetben előírt alkalmakként kötelezően rendelték el harckészültségi gyakorlatokat, melyeket röviden riadónak neveztek, ugyanis ezzel a jelszóval jelezték a katonáknak a feladatok megkezdését. Az elrendelés legtöbbször hajnaltájt történt. A városban lakó tiszteket elsősorban telefonon riasztották, majd egy adott ponton gépkocsi várta őket. Így volt ez megszerveve az akadémián is. Bár a közlekedés már akadozott, a villamosok nem indultak, az állomány az előírt időre beért.

Minden riadóterv első mozzanata, hogy meg kell kezdeni a laktanya védelmének az ellátását. Ehhez fel kell venni a megfelelő fegyvereket és az azokhoz járó lőszeret. Az akadémia megkettőzte az őrséget, megerősítette az ügyeletes alegységet, és a kapuval szemben felállította a géppuskát. Megkezdtek a laktanya körül a járőrözést. Mivel az akadémiának jelentős fegyverzet nem állt rendelkezésre, első feladatként 24-én - a *Politikai Főcsoportfőnökségtől kapott javaslat alapján* - gépkocsival szimpátia felvonulást terveztek, zászlókkal, és hangos énekléssel. A közeledő katonai oszlopot azonban az Orczy térnél megtámadták, amire nem számítottak. A géppuskatűz hatására megálltak, majd alkudozásba kezdtek a civil fegyveresekkel, akiket megnyugtattak, hogy ők is a forradalom mellett állnak, és mellette tüntetnek. Ezután elengedték őket, de nem jutottak messzire. A Körútnál ismét fegyveresek állították meg az oszlopot. Ekkor az akadémia parancsnoka "beszédet intézett a felkelőkhöz", és a menet céljául a szovjet parancsnokságot jelölte meg, ahova tárgyalni indultak. Ekkor a felkelők közölték, hogy néhány orosz fogoly van birtokukban. Márton ezredes kijelölte Nagy Tibor alezredest, hogy vegye át a foglyokat. Így a foglyok a Zrínyi akadémiára kerültek.

Október 24-én beérkezett az akadémiára az *aszódi gépesített lövészezred* állományának egy része, akik a laktanyában kaptak elhelyezést. Több bevetésben is részt vettek, de mire a helyszínekre értek, már mindenhol elhelyezték.

Feladatok a rendszer intézményeinek védelmében

Tekintettel a politikai helyzetre, a "rendcsináláshoz" önkénteseket kértek az akadémián. Közölték velük, hogy kis létszámú rendszerellenes elemek, fegyveres támadást intéztek néhány objektum ellen. Ezeket az objektumokat kell visszafoglalni. Az egyik csoportot ötven fővel a Danuvia fegyvergyárhoz írá-

nyitották. Mire az akadémiai hallgatók odaértek, a felkelők már kiürítették a fegyver és lőszerraktárt.

A Zách utcában (ez az akadémia mögött van, csak egy utca választotta el a két intézményt) a hadtáp tisztí iskolának az őrségét a felkelők lefegyverezték. Az akadémiáról indított felmentő csapatnak a laktanyát sikerült visszafoglalni, és a lőszerraktárból a lőszert átszállítani.

Az akadémia 60 főt irányított a XIV. kerületi rendőrkapitányságra, melyet a felkelők megtámadtak. A csoport élén az egyetlen működő harckocsi haladt. A rendőrörsöt felmentették, a harcban senki nem sérült meg. Egy másik nagyobb csoportot a SZABAD NÉP székház védelmére rendelték ki a Blaha Lujza térre. Az újság ekkor a Magyar Dolgozók Pártjának a központi lapjaként íródott. A szerkesztőséget már előző este megtámadták, mivel a követeléseiket nem akarták kinyomtatni, törni, zúzni kezdtek, néhány szerkesztőt megvertek. Másnap az újság nem is jelent meg. A harci csoport azt a feladatot kapta, hogy foglalja vissza a Szabad Nép székházat. A csoport parancsnoka Dienes Ödön ezredes, helyettese Derestei Sándor alezredes, politikai helyettese Unger Endre alezredes. A védelemre kiküldött csoport előtt az akadémia egyetlen T-34-es típusú harckocsija haladt, azt követték a tehergépkocsik, melyek a tiszteket szállították. A kedvező megközelítés érdekében a harckocsi tornyára kitűzték a magyar zászlót. A menetet egy golyószóróval Urbán Vilmos százados biztosította. Irányzó helyettese Kovács Lajos százados, lőszeres Sági Sándor őrnagy.

A megjelenő magyar katonákat a Népszínház utcában éljenzéssel fogadták, bár kisebb incidens hatására néhányan püfölni kezdtek. Ekkor már látszottak az események maradványai. A körút kereszteződésében feküdt a ledöntött Sztálin szobor egy darabja, távolabb egy feldöntött villamos és egy még égő szovjet páncélgépkocsi is látszott. Az akadémia tisztjei kisebb csoportokban elfoglalták a székházzal szemben lévő Nemzeti Színházat, majd a megüresedett székházat és a hozzá tartozó épületrészt. Ekkor már a földszinti könyvesbolt kiégett maradványai és a kiszórt könyvek jelezték, hogy itt az éjjel komoly cselekmények történhettek.

Október 25-én tömeg a Nemzeti Színház előtti téren gyülekezett és jelszavakat skandálva szidták a katonákat. (a régi, lebontott színházról van szó) Egy csoport erőszakkal kívánt az épületbe behatolni, azzal a céllal, hogy az újság nyomtassa ki követeléseiket. A kirendelt parancsnok tűzparancsot adott, mire vita támadt a hallgatók között arról, hogy lőjenek vagy ne? Miközben folyt a vita, egy véletlen eseménynek köszönhetően tűzharc fejlődött ki.

A Népszínház utca és a Körút sarkán, egy több BTR-152-es nyitott tejetű páncélgépkocsikban szovjet katonák állomásoztak. A Nemzeti Szállót megszálló civil fegyveresek közül valakik rálöttek a katonákra. Ekkor a székház tetején figyelő Kovai Sándor őrnagy vaktában elkezdett lövöldözni, mire a szovjet lövészek elindultak a Rákóczi tér irányába. Nem telt el sok idő, egy

harcokocsival érkeztek vissza, aki tüzet nyitott a székházra. A színház nyitott ablakában lévő géppuskát meglátva, oda is lőtt egy gránátot. A kezelők alig tudtak elmenekülni. Ezután vad lövöldözés kezdődött minden irányból. A végeredmény: a szovjetek szétlőtték a színház egy részét, az EMKE szállót, az Éjjel-nappal Közértet. A környező épületek földszintjeit szitává lőtték a páncélgépkocsik géppuskái. A magyarok ezt nem nézték tétlenül, és a tovább haladni akaró csoportot Derestei alezredes megállította, géppisztolyával megdöngette a harcokcsi oldalát, mire a nyílásban megjelenő parancsnoktól megkérdezte: miért lövik a székházat? Mire azt a választ kapta, hogy a halott két katonáért!

Miután megbeszélték hogy itt magyar tisztek védelmezik a környéket és együtt kell működniük, a továbbiakban az idő nyugodtan telt. A tisztekről nem gondoskodtak, nem kaptak ételmezt, és a köpenyeiket is csak 27-én hozták ki.

A korábbi lövöldözés híre elterjedt a városban és még nagyobb tömeg gyűlt össze a székház és a színház közötti téren. Végül a nyomda vezetése úgy döntött, hogy enged a követeléseknek, és beengedi az ifjúság küldötteit. A küldöttséggel együtt, benyomultak a fegyveresek is, mögöttük a tömeggel, és elfoglalták az épület egy részét. Ezután barátkozás kezdődött, és a beszélgetésből kiderült, hogy mi a felkelők célja. A védők tudomására jutott, hogy megalakult az új kormány és tűzszünetet rendelt el. A kihelyezett csoportot 28-án visszarendelték az akadémiára, ahová néhány lemaradt tisztet kivéve meg is érkeztek. Ebben a tevékenységben főként az akadémia összefegyvernemi tanszéke és hallgatói vettek részt. A Szabad Nép székházát ezután egy fegyveres csoport szállta meg, melynek Dudás József volt a vezetője. Az épület lett a csoport állandó tartózkodási bázisa. Visszafoglalására még egy kísérletet tettek egy rendőri csoporttal, melyet Kopácsi Sándor budapesti rendőrkapitány vezetett, de a túlerőben lévő felkelők körülfogták a csoportot, mire Kopácsiék tárgyalásokba kezdtek, végül békésen eltávozhattak. Ebben a szerkesztőségben íródott aztán a híres vezércikk a „Hajnalodik,” melyből megtudhatták az olvasók, hogy Budapesten igazságos felkelés tört ki, akik ebben részt vettek nemzeti hősként. Akik eddig a régi rendszert védelmezték megtévedtek, a szovjetek és az államvédelmisták pedig az ellenségeink.

Telefonközpontok védelme

Az akadémia egy kisebb csoportot indított útba a *Krisztina telefonközpont* védelmére. A távbeszélő központok ezekben az években fontos katonai objektumok voltak. Az együttműködést a Posta Katonai Szolgálat biztosította, amely az adott postán kapott elhelyezést. Ennek a védelme is fontos katonai feladat volt. A fő feladatot a Híradó tanszék beosztottjai kapták, mint akik szakmailag is ismerték az objektumot. A telefonközpontot határőrökkel is megerősítették, a budapesti határőr-híradókat is kiképző központjából. A vé-

dőknek a többszöri fegyveres támadás ellenére, sikerült a központot október 30-ig megtartani. Ezután alkudozás kezdődött, és a központot további őrzésre november 2-án átadták a kijelölt nemzetőr csoportnak, és bevonultak az akadémiaira.

A nemzetközi összeköttetéseket lebonyolító *József telefonközpont* is fontos védelmi góc volt, melyet a 102. rádió-felderítő ezred egy csoportja védett, Gyuricza Imre híradó alezredes parancsnoksága alatt, kiegészítve az akadémistákkal. A központot négy szovjet harckocsi is védte. Ezt a központot is támadták a fegyveresek, például rálöttek a szovjet katonákra a közeli templom tornyából. A járőr elfogta a lövöldözőt, aki egy fiatal gyerek volt. Amikor a szovjet harckocsik parancsot kaptak, hogy ki kell vonulni Budapestről, akkor a nagy kapkodásban a központban felejtettek egy szovjet főhadnagyot, és a Romániából idevezényelt 33. motorizált alakulattól itt ragadt 3 szovjet "harcost", akik a Corvin-köznél elvesztették csapatukat és ide hozták őket. Innen vitte ki őket Tököltre Fomin alezredes, aki akkor a Különleges Hadtestnél volt tolmács.

Az akadémia több kisebb feladatot is teljesített. Ilyen volt a kecskeméti lövészezzreddel közösen végrehajtott feladat. Azt a parancsot kapták, hogy a HM közelében lévő tiszti lakásokat védjék meg. A csoport élén az egyetlen harckocsi haladt, melyet Pacsek József százados (később vezérőrnagyként csoportfőnök) irányított. Másik feladat a Kőbányai vasútállomásra érkező Miskolci vonat átkutatása. Az előző értesítés szerint ezen felkelők utaztak a fővárosba. Itt szervezatlenségből két polgári utas kapott halálos lövést. A vonaton forradalmárokat nem találtak. *Itt kell megjegyeznem*, a Néphadsereg tagjai részére a " választóvíz " a már említett Szabad Nép cikke a HAJNALODIK volt, amely az eddigi eseményeket népfelkelésnek nevezte, így a kirendelt intézmények és alakulatok, akik fegyveresen védték a " néphatalmat " nem tartoznak a forradalmárok közé. Hogy a további összetűzéseket elkerüljék, a parancsnokok feladták a védendő objektumokat, és visszatértek a laktanyákba.

A Szabad Nép vezércikkéből - *ami az akkori egyetlen pártnak a Magyar Dolgozók Pártjának a hivatalos lapja volt* - az is kiderült, akik eddig a hatalmat védték, azok lettek a népellenesek, akik ellene felléptek, azok lettek a nép akaratát végrehajtó forradalmárok.

A forradalom második szakaszában a hadsereg az új kormány határozatának megfelelően tagja lett a megalakult Nemzetőrségnek. Egyes alakulatai az új honvédelmi miniszter - *Janza Károly altábornagy* - parancsai szerint cselekedtek. Ennek a parancsnak a lényege az volt, hogy a hatalmat a fegyveres erőkből és a felkelőkből alakult forradalmi egységek közösen gyakorolják. Ennek érdekében azokat is fel kellett fegyverezni, akiknél eddig nem voltak fegyverek. A forradalmi eseményekben szétszóródott alakulatok beosztottjainak gyülekezési körletet jelöltek ki október 25-étől a Zrínyi Akadémián és a

Kossuth tüzér tiszti iskolán. A bevonulók részletesen ecsetelték az eseményeket, egyéniségüktől függően hol hősként, hol áldozatként tüntették fel magukat. Legtöbbször a katonai felső vezetést hibáztatták, nemcsak azért mert a löszert nem osztották ki időben, hanem elmarasztalták őket az együttműködés megszervezésének az elmaradásáért, az egymásnak ellentmondó parancsok kiadásáért is. Ily módon rontották a velük érintkező tisztek morális helyzetét és kedvezőtlenül hatottak a kapott feladatok ellátására. Többször okoztak tüzpárbajt egymás ellen.

Megalakul a nemzetőrség

Az új honvédelmi miniszter, Janza Károly altábornagy kiadott parancsa értelmében október 29-től az akadémián is megalakult a Nemzetőrség. Ez lényegében azt jelentette, hogy az akadémia tagjai nemzetőr igazolványt kaptak, amivel igazolhatták, hogy ők a Magyar Nemzetőrség tagjai. Ugyanilyen módon lettek tagjai a tiszti iskolák beosztottjai és növendékei a nemzetőrségnek. Ilyen alapon tehát, 1956-ban minden tisztt, tiszthelyettes, és növendék nemzetőr volt. Az igazolványt az új parancsnok, Király Béla vezérőrnagy írta alá. Ez egy kartonlap volt, áthúzva piros-fehér-zöld csíkkal, és igazolta, hogy X Y a nemzetőrség tagja.

Akadémisták és a Corvin-köz

A legtöbbet vitatott esemény a Corvin-közben és környékén lévő fegyveresekkel történő együttműködés volt, mely katonai részről főleg a Zrínyi Akadémiát érintette.

A legnagyobb ellenállást Budapesten a Corvin-köztől elnevezett csoport fejtette ki, melynek alcsoportja a Práter utcai iskolában volt. Ennek a csoportnak a megsemmisítésére kívánták bevonni az akadémiát, egy szovjet rohamcsoport támogatásával október 24-én. Az akadémiának együtt kellett összeállítani a rohamcsoportot a közben Kecskemétről beérkezett 12. gépesített ezredből. Tóth Zoltán alezredest a Honvédelmi Minisztériumban eligazították a feladat végrehajtására, megszervezték a szovjetekkel a találkozót és az együttműködést. Mikor Tóth elmondta Márton ezredesnek a támadás tervét, amely szerint a gyalogságot a magyarok adják, a szovjetek pedig csak tüzérségi tüzellel támogatnak, valamint páncélos erőket adnak, akkor Márton úgy döntött, hogy ilyen terv mellett csak a magyarok pusztulása várható, és kérte az akció elhalasztását. Janza vezérőrnagy nem fogadta el Márton érvelését, és parancsot adott az eredeti terv végrehajtására. A hadműveleti csoportfőnökség kijelölte iránytisztnak Szentesi Ede alezredest, aki megjelent az akadémián. Eligazításra október 27-én kellett jelentkeznie Márton ezredesnek a Dimitrov téren berendezkedett szovjet parancsnokságon. 28-ára a terv szerint légi és tüzérségi tüzellel előkészített támadást terveztek a Kilián laktanya és a környező épületek ellen. Az eligazítás után Márton elhatározta, hogy elmegy a Cor-

vin-közbe és figyelmezteti az ott lévőket. Amikor megismerkedett az ott lévő személyekkel, és a csoport céljával ígéretet tett, hogy jelenti a szovjetek tervét Nagy Imre miniszterelnöknek. Csak Hegedűs Andrással sikerült beszélnie, aki megígérte, hogy átadja az üzenetet Nagy Imrének, aki akkor a kormányfő volt.

Mivel ellenkező parancs nem érkezett 28-án hajnalban a kijelölt akadémista csoport egy harckocsival az élen elindult a feladat végrehajtására. A támogatásra kijelölt kecskeméti gépesített lövészezreddel nem jött össze a találkozó. Azok a szovjet harckocsik, amelyek szintén csatlakoztak volna, már az Üllői út- Nagykörút kereszteződésében elakadtak, (megsemmisültek) az ott lévő erők támadásának köszönhetően. Vita támadt a szovjetekkel nemcsak a támadási tervről, hanem annak módjáról is. A magyarokat ugyanis a nyitott páncélgépkocsikkal kívánták a szovjetek a helyszínre szállítani, amibe Márton nem ment bele. Ekkor ugyanis már közismert volt, hogy a legtöbb ilyen nyitott eszközbe fölülről egyszerűen a felkelők bedobtak egy benzines palackot, és a benne ülők megégték. Voltak még más problémák is. Például a rohamcsoportok és a harckocsik között nem volt rádióösszeköttetés, mert nem voltak erre eszközök. Ennyi probléma láttán az ott lévő parancsnokok, Marton ezredes, Szűcs Miklós ezredes, Kovács alezredes és Tóth alezredes kérték a támadás elhalasztását a szovjettektől. A szovjet hadtestparancsnok ezt nem fogadta el, kiadta a támadási parancsot. Több harckocsit küldtek ki felderítés céljából, akik nem érkeztek vissza a Corvin-közből. Ilyen helyzetben a parancsnok úgy határozott, hogy visszavonulnak a bázisukra. A magyar erők este 8 órára beérkeztek az akadémiára. Marton visszaérkezése után kapta csak meg Nagy Imre miniszterelnök üzenetét, melyben a Corvin-köz fegyveres felszámolását megtiltotta. A támadás megismétlését a szovjetek 29-ére tervezték, de ezt a magyarok már nem támogatták.

Márton ezredesnek ezt a tettét később, a felelőségre vonások idején, súlyosbító körülményként értékelték.

Az akadémia „szomszédai”

Az akadémiának voltak „összetűzései” az intézet melletti Szamuely Tiborról elnevezett államvédelmi erőket állomásoztató laktanyával is. Annak parancsnoka Orbán Miklós államvédelmi ezredes volt. Közismert, hogy a népharag első számú célpontjai az államvédelem volt. Ezért attól félve, hogy a laktanyában lakó családtagokat bántalmazni fogják a felkelők, azt kérték, hogy átmehessenek a Zrínyire. A parancsnok befogadta őket, és az egészségügyi objektumban kaptak szállást. A laktanyájukat a későbbi események hatására az államvédelmisták elhagyták. Őrzéséről az akadémia gondoskodott. Később ezt úgy állították be, hogy a Zrínyi elfoglalta az államvédelem laktanyáját.

Az akadémia miután felvette a kapcsolatot a Corvin-közzel, a felkelőknek ennek a laktanyának a készletéből utalt ki fegyvereket és más katonai felszereléseket. A másik szomszédos laktanya, amely régebben a

BEM légvédelmi tüzér tiszti iskola volt, és 1956 szeptemberéig a hadtáp tiszti iskolának adott otthont, - az akadémia kezelése alá tartozott. Itt helyezték el a vezényelt csapatokat, és ezt szállták meg november 4-e után a szovjet páncélosok.

Az akadémia tisztjei a Corvinisták között

Az anyagi segítségen kívül a Corvin-köziek szellemi segítséget is kértek. Kiképzésükre október 30-án 12 tiszt indult a helyszínre. A csoport parancsnoka Dienes Ödön ezredes főtanár volt. Megérkezvén a Corvin-közbbe, kiosztották az új Nemzetőri Igazolványokat. Nemzetőrségnek tagjai lettek a forradalmárok is. Az akadémiával a rádiós kapcsolatot Haász János százados főtanár által telepített rádión és a postai távbeszélőn tartották. Fő feladatuk az ott összegyűlt polgári személyek szakszerű, rövid idejű kiképzése volt, a Nemzetőrségben adódó feladataik ellátására. A rádióállomás kezelője Orosz Mihály híradó hallgató és még két társa lett. A megszervezett rádióhálóba bekerült még a Budaörsi híradó ezred, és Ferihegy. A kiképzésnek a november 4-i hajnali támadás vetett véget. Az eseményekben résztvevő akadémisták egy része, látva a komoly veszélyt, a felelőségre vonás elől külföldre távozott. Ilyen volt Arnóczky Pál híradó százados és Haász János százados, akik lelkes hívei lettek a kialakuló új rendnek. Arnóczky tagja lett az akadémia Forradalmi Bizottságának is. Márton András visszaemlékezésében megemlíti, hogy - Márton forradalomban betöltött szerepét ismerve-, megjelent egy teherautóval, és kérte, hogy ő is távozzon külföldre. Márton ezt nem fogadta el, és az akadémián maradt.

Márton ezredes október 31 - én délelőtt részt vett a Corvin-közi csapatok Parancsnokválasztásában is. Ekkor választották meg Iván-Kovács helyett Pongrácz Gergelyt, akit Márton is támogatott.

Ezután, mint az akadémia parancsnokát meghívták a honvédelmi minisztériumban tartandó értekezletre, melynek az volt a célja, hogy megválasszák a Honvédelmi Forradalmi Bizottságot. Ebbe beválasztották, és őt nevezték ki Budapest védelmi parancsnokának. Akadémia parancsnoki utódjáról is gondoskodtak, Székely Béla vezérőrnagyot kinevezték az akadémia új parancsnokának. A Corvin-közbbe a honvédség javaslata az volt, hogy a 18 év alatti fegyveres fiatalokat le kell fegyverezni. Helyükre a Zrínyi akadémia 400 főt biztosít, akik mint szakképzett katonák átveszik a parancsnoki beosztásokat. Pongráczék ebbe sem mentek bele, végül abban maradtak, hogy a tisztek és a forradalmárok kinevezett parancsnokai együtt vezetik az alegységeket.

Október 30-án sor került a Corvin-köz parancsnokának a újráválasztására, mert a régi parancsnokot azzal gyanúsították, hogy államvédelmista besúgó. A Corvin mozi előtt összegyűlt szabadságharcosokhoz az emeleti parancsnoki iroda ablakából Márton ezredes mondott beszédet:

„Bajtársak ! Győzött a forradalom, és ebben a Corvinistáknak óriási szerepük volt. A szovjet csapatok elhagyták Budapestet, és rövidesen kivonulnak az ország többi területéről is. A ti hősi küzdelmetek előtt nemcsak az ország, hanem a világ összes népei meghajtják fejüket, mert ti a Pesti Srácok, történelmet írtatok. Amikor szükség volt rátok, tudtátok hol a helyetek. Most azonban a legsürgősebb feladat, hogy megvédjük azt amit oly sok vér árán kivívtunk. Helyre kell állítani a rendet és a Nemzetőrségen belül, a rend fenntartása is rátok hárul. Éppen ezért főparancsnokra van szükségetek, aki a parancsnokok által erre a tisztségre jelölt négy bajtársatok közül kell megválasztanotok.” Ezt a beszédet később a bíróság úgy értékelte, mint uszító felhívást. A választáson jelen voltak még: az akadémiáról Laskó László őrnagy, Zentai Gyula alezredes, Dienes Ödön ezredes, Hámori Ferenc alezredes, Fodor Gyula, Lipták László őrnagy, Damó László, Kindlovics Pál, Jónás Tivadar századosok. A Corvin köz több csoportot foglalt magába, melynek az irányítása és feladatszabása a főparancsnok és törzse feladata volt. Irányítása alá tartozott mintegy 1000 fő szabadságharcos. (Molnár János cikke a Történelmi Társulat folyóiratában)

Őrség a parlamentben

Október 27-én a Szabad Nép székháztól visszatért állománnyal közölték, hogy az új kormány őrzését kapják feladatul. A feladatra az összefegyvernemi tanszék állományából választották ki a tiszteket akik rendbe hozták magukat, összeállították felszerelésüket, és löszert vételeztek. Fegyverük pisztoly és géppisztoly volt. A parancsnok Unger Endre alezredes lett. A csoport gépkocsival ment a parlamentbe. A feladat ellátására azért volt szükség, mert a parlamenti őrséget, - mint az államvédelemhez tartozó egységet - feloszlatták, és a parlament őrizetlenül maradt. A mintegy 25 főből álló tiszti különítmény feladatai szerteágazóak és felelősségteljesek voltak. Ők látták el a kapukban a belépéshez szükséges igazoltatásokat, egyeztették a belépéshez szükséges jogot. Tárolták a belépőktől elvett fegyvereket. Kisérték a fontos személyeket, állami és pártvezetőket, a kormány tagjait, védték őket az esetleges atrocitásoktól és a molesztálásoktól. Tartották a kapcsolatot a parlament külső védőivel.

Futárszolgálatot is elláttak, bizalmas iratokat továbbítottak. A kormány tagjaihoz csak az arra kijelölt kapun keresztül lehetett bejutni. Erre a célra három bejáratot jelöltek ki. A Kossuth híd (ma már nincs meg a híd, lebontották, volt bejáratánál van József Attila szobra) felőli kapun lehetett bejutni például Tildy Zoltán államminiszterhez, Kádár János pártfőtitkárhoz. A legtöbb küldöttség Tildy államminiszter urat kereste. Tildy Zoltán volt köztársasági elnöknek megjelent a régi személyi testőre Keresztes János őrnagy, akinek csak a régi egyenruhája volt meg, ezért azt vette fel. Erről írtak később úgy, hogy “Horthysta tisztek” vették át a hatalmat a parlamentben. Bár ő és néhány

később beérkezett régi tisztt foglalkozott egy új parlamenti őrség megszervezésével, de erre nem került sor. Egy akkoriban megjelent napilap novemberi 3-i száma arról tudósított, hogy új Parlamenti őrség vette át a képviselőház őrzését, melyet korszerű fegyverekkel láttak el. Az "új" mindössze az volt, hogy a tisztek megkapták a Bocskai-sapkát, az új rendfokozati jelzéseket lecserélték, a régi sapkarózsát kicserélték, és egymást elvtárs helyett, Bajtárs !-nak szólították..

November 4-én vasárnap, kevesen tartózkodtak a parlamentben. Előző este a legtöbb miniszter hazament, már csend uralkodott a városban, biztonságosan lehetett közlekedni. Amikor hajnalban a szovjet csapatok megindították Budapest ellen a támadást, már hallatszottak az ágyúlövések. Nemsokára szovjet harckocsik vették körül a parlamentet. Az akadémistákat lefegyverezték, majd egy szobában őrizték őket egy napig. Unger Endre alezredes felháborodására először a tiszteket, később a sorkatonákat is elengedték.

Mi történt az akadémián ?

Márton ezredes november 3-án tiszti gyűlést hívott össze az akadémián. A bent lévő állományt tájékoztatta a szovjet csapatok Budapestről történő kivonulásáról, és arról a határozatról, amelyben döntés született, hogy tárgyalásokat kezdett a további csapatkivonások megtervezéséről és megszervezéséről. A további tevékenységről és az akadémia feladatairól elmondta, hogy nincs kapcsolata a honvédelmi vezetéssel, így nem tudja mi lesz a feladatuk. Egy hallgatói kérdésre, miszerint mi lesz ha nem mennek ki az oroszok, azt válaszolta, " hogy akkor az aggoktól a csecsemőkig mindenki fegyvert fog a magyar szabadság érdekében."

November 4-én hajnalban felhívta Király Béla telefonon (ő volt a Nemzetőrség parancsnoka) hogy a szovjetek támadást indítottak nemcsak Budapest, hanem az ország összes laktanyája ellen. Közölte, hogy törzsét áthelyezi Budára. Aznap reggel Pongrácz Gergely a Corvin-köziek parancsnoka jelentkezett az akadémián és Mártont kereste. A parancsnok lement a kapuhoz. Pongrácz tanácsot kért a további tevékenységhez. Az ő elképzelése az volt, hogy embereivel visszavonul a Bakonyba és partizánharcot folytat. Márton ezt ellenezte, és azt tanácsolta, hogy ő és a csoportja vonuljon illegalitásba.

A szovjet harckocsik reggel nyolc óra tájban érkeztek az akadémia elé. A szovjet tiszte Márton orosz nyelven megszólalva fogadta, ami meglepetést keltett, valószínűleg az eligazítás alapján nem erre számított. A szovjet tisztt közölte hogy az a parancs, hogy le kell fegyvereznie a laktanyában tartózkodókat. Miután közölték vele, hogy itt csak személyi fegyverek vannak, némi vita után eltávozott. Az akadémiát egyenlőre békén hagyták. A helyzetet kihasználva ezután a tisztek többsége hazament.

Ettől az időponttól kezdve új fejezet kezdődött az akadémia életében.

Tessedik Tamás:

Az információ biztonság stratégiai menedzsmentje
(PHD hallgató, ZMNE)

Bevezetés

A távbeszélő szolgáltatóknak soha eddig nem látott feladatokat kell ellátni a piaci funkcióik mellett nemzetbiztonsága rendvédelme, nemzetvédelme és katasztrófa elhárítása terén. Ki kell hangsúlyoznom, hogy a piacgazdaság és a védelem politika között folyamatosan fejlődő és egymásra ható új viszonyrendszer kezd kialakulni. Rá kívánok mutatni a piaci viszonyok között működő, és egyben nemzeti érdekeket is képviselő objektumok, vállalkozások nemzetvédelmi és nemzetbiztonsági feladataira, ezen társaságok egyensúlyi törekvéseire a piaci és a nemzeti követelmények között. Az elektronikus hírközlési vállalatok, mint piaci szereplők új típusú közreműködései a védelmi és biztonsági feladatok ellátása terén.

Gondolatok a távközlési szereplő biztonsági feladatairól

1. A hírközlés technikai és szervezési rendszerének történeti áttekintése, fejlődési irányzatai

Ahhoz, hogy teljes képet lehessen kialakítani a hírközlési és informatikai rendszerek fejlődési útjáról nem kerülhető meg, hogy szerepüket a védelmi szférában összefoglaljuk. Ennek részét képezi a hírközlés nemzeti stratégiai momentumai, az alkalmazott szervezet fejlesztési és megvalósítási módszerei. Ezek az alábbi pontok szerint foglalhatóak össze:

- 1.1. Technikai rendszerek fizikai megvalósításának meghatározása. A 2. és 3. generációs távközlési rendszerek üzembiztonsági modelljei.
- 1.2. Nemzetközi ajánlások, szabványok és módszerek bemutatása.
- 1.3. A műszaki és szervezési módszerek fejlődéséből leszűrhető rész következtetések extrapolációval, a következtetéseket befolyásoló kockázati tényezők.

2. A hírközlés törvényi alapjai és a generációs fejlődésekkel harmonizáló törvényi rendek várható alakulása

A távközlő rendszerek üzemben tartását bonyolult jogrendszer szabályozza. Ezért elkerülhetetlen összefoglalni mindazokat a jelenleg hatályos jogszabályokat, amelyek alapjaiban határozzák meg a szolgáltatóval szemben támasztott követelményeket, kötelezettségeket. Természetesen folyamatosan szem előtt tartva a szolgáltató elsődleges funkcióját. Miközben a hírközlési piacon eleget kell tennie a tulajdonosi elvárásoknak, egyben eleget kell tennie a nemzetvédelmi és biz-

tonsági, valamint rendvédelmi kötelezettségeinek is. A fejezet az alábbi alfejezetek szerint kerül kidolgozásra

- 2.1. A hírközlést nemzetközi és hazai jogszabályi rendszere, a végrehajtásokat meghatározó kormányrendeletek összefoglalása.
- 2.2. A nemzetközi irodalom által meghatározott biztonsági szabványok ismertetése, azok egymáshoz való viszonya. Az egyes minőség biztonsági szabvány megoldások erős és gyenge pontjai, esetleges hiányosságai.
- 2.3. A távközlő rendszerekben keletkező adatok, információk informatikai védelme. A személyi és adatvédelem prioritása.
- 2.4. A törvényi szabályozásokat befolyásoló jövőbeli tényezők, és az azokból levonható részkövetkeztetések.

A hírközlési szereplők (stake holderek) egymáshoz való viszonya. Vertikális integrációk, horizontális kapcsolódások, stratégiai szintek, szövetségek, stb viszonyok elemzése. A közreműködők folyamatosan alakítják ki részvételi formájukat a távközlési és az informatikai piacon, miközben keresik annak szükséges egyensúlyát, ami segít az egymással kölcsönhatásban álló két önálló tudomány, az egyes fejlődési szintek (vertikális) integrációs eredményeinek, valamint az egyes technikai megoldások (horizontális) gyakorlati megjelenésének gyakorlati alkalmazhatóságában. E téma körben az alábbi néhány gondolattal elkerülhetetlenül szembe kell nézni:

- 2.5. A mobil távközlő rendszerekbe integrálódó informatikai rendszerek.
- 2.6. A hírközlés és az informatika statikus konvergencia rendszer modell módszerének kidolgozása. A levonandó részkövetkeztetések meghatározása.

A stake holderek stratégiai szövetségeinek biztonság menedzsment szerinti megközelítése. Biztonságmenedzsment feladatok az integrációk különböző szintjein.

3. A vizsgált rendszer elemek betörési pontjai (gyenge pontjai), és az ellenük való védelem szervezési és informatikai szempontrendszerei

A fejezet célja a statikus elemzésen alapuló dinamikus vizsgálatok kutatási eredményeinek összefoglalása, melyek meghatározzák a technikai alapú döntés előkészítések determinisztikus és stohasztikus szintjeit. Rá kívánok mutatni a döntési mechanizmus kockázatkezelési módszereire a távközlő rendszerek betörés elleni védelmének biztosítása kapcsán.

A fejezet az alábbi alfejezetek szerint kerül kidolgozásra

- 3.1. Javaslatok kidolgozása a távközlő rendszerek működési biztonságának megvalósítására. A hírközlő rendszerek működésének folyamat-szervezése. A fő- mellék és kiegészítő folyamatok rendszer szervezési elméletének kidolgozása.
- 3.2. A biztonsági menedzsment stratégiai szempontrendszerének meghatározása. A komplex dinamikus modell módszer időbeni alakulásának leírása.

4. A megvalósítási lehetőségek költség-haszon vizsgálata

A legkorszerűbb döntéshozatal sem kerülheti meg az intézkedés procedúrájával együtt járó a pénzügyi vizsgálatokat sem. A fejezet célja azon alkalmazási módszerek összefoglalása, melyek mérni képesek az információ jövedelmezőségeit, képesek pontosan számszerűsíteni, illetve alkalmasak a döntési költségek meghatározására. Rá kívánok világítani az egyes biztonsági funkciók megvalósításával összefüggő költségek optimalizálására, melyeknek minden esetben egyensúlyban kell lennie a távközlő rendszer technikai feladataival és a rendszer céljával.

A fejezet az alábbi alfejezetek szerint kerül kidolgozásra

5.1 A hírközlő rendszeren forgalmazott információ jövedelmének meghatározása. Az információ jövedelem anyagi kifejezése. A védelmi technológia kialakításának szempontrendszere:

1. célorientált védelmi rendszer,
2. érzékenység vizsgálat a generációs változásokra,
3. beruházási és üzemi költségelemek a stratégiai döntéshozó szempontjából.

5.2 Javaslat a technikai, informatikai és költség-haszon elemek viszonyrendszerének leírására mind a statikus, mind a dinamikus platformon.

További gondolatok a az információ biztonságot érintő feladatok kezeléséhez

A választott téma hatványozottabban időszerű, mint azt csak sejteni is lehetett bármikor. Az elhírhedt 2001 szeptember 11.-i terror támadás óta a nemzet biztonságának kérdése hazánkban is a társadalmi érdeklődés elvárások homlokterébe került. Dolgozatom téma választásakor is már ismert volt az az alap tézis, hogy korunk új jövedelem termelő tényezője az információ, melynek hordozói nemzeti stratégiai kérdés. Ezért azok védelme nemzetbiztonsági illetve nemzetvédelmi szempontból kiemelkedő jelentőséggel bír. Az információt továbbító telekommunikációs eszközrendszerek biztonsági szempontú vizsgálata számos ma már kidolgozott módszereken alapuló elemzéseket igényelnek, melyek az alábbi célrendszerben kerültek megfogalmazásra:

- a távközlés és az informatika integrálódási folyamatainak bemutatása, e
- rendszerek fejlődési trendjeiből levonható tudományos eredmények rendszerezése és extrapolatív következtetések levonása,

- a távközlő rendszerek fejlesztésével és működtetésével összefüggő fő és kiegészítő folyamatok szervezési és vezetési szempontrendszerének kidolgozása védelmi és biztonsági aspektusból,
- a folyamat fázisainak viszonylatában vizsgált technikai rendszerelemek statikus és dinamikus modelljeinek kidolgozása (E célrendszerben az alábbi kérdésekre adott válaszokat kell kidolgozni:
 - o kockázati tényezők meghatározása,
 - o a hazai és a nemzetközi, elsősorban az EU biztonság menedzsmenti állásfoglalások, biztonsági akarat és a hírközlési liberalizáció egyensúlyi feladatai,
 - o gazdasági tényezők vizsgálata a költség - haszon tükrében,
 - o a frusztrációra való reagáló képesség meghatározása és a tényezők optimum analízise (stratégiai flexibilitás mérése kvantitatív módszerrel),

Míg a célfüggvény független változói egyértelműen definiálhatóak, addig a környezetet leíró függvény függetlenváltozóinak számáról csak az jelenthető ki, hogy típusai jól körül határolhatóak. Ezért a környezeti függvények esetében környezeti függvény halmazról beszélhetünk, melyeket $K_1, K_2, \dots, K_m$ -el is jelölhetünk.

A K környezeti függvény gyakorlati megjelenési formája tulajdonképpen a függetlenváltozóknak a mindenkor T időben vett aktuális kombinációjából ered. Ez matematikai eszközökkel leírva:

$$K = K(a(T); b(T); \dots, k(T))$$

Ahol az $a, b, \dots, k$ függetlenváltozók a mindenkor T időben a 0 és 1 közötti értékkel szorzódnak. E tényező figyelembe vételével a fenti összefüggés az alábbiak szerint alakul:

$$K_T = K_T(a_T(a); b_T(a); \dots, k_T(a))$$

ahol az $a = 0, \dots, 1$ közötti érték,

Tehát a K környezeti függvény egy olyan függetlenváltozók által generált több változós függvény, mely esetben a függetlenváltozóinak eredő vektorai nincsenek, hatásukat a szuperpozíció útján fejtik ki.

A környezeti függvénynek a függetlenváltozói lehetnek determinisztikusak és sztohasztikusak. Determinisztikus minden olyan eset, amely előre és egzakt matematikai eszközökkel leírható. Ezek közé tartoznak pl. a telekommunikációs verzió váltással járó technikai átállások kvantitatív mérőszámainak leírása, vagy az előre tervezett technikai áttelepüléssel járó átmeneti kapacitás korlátozásból eredő információ kiesés veszteség mértékének meghatározása.

Vizsgálva a biztonsági stratégiai függvényt a stratégiai tervezés rendszerében, az alábbi matematikai összefüggés írható fel:

$$Stfoly.=Stf(S(C \times K));$$

Ugyanez más megfogalmazásban:

$$STfoly.=STf1;STf2;....STfm$$

Ahol az STfm a stratégiai tervezés az életgörbe m-ik fázisában.

Ennek figyelembe vételével a célfüggvény x ; y függetlenváltozóinak az életgörbék során lejátszódó fő és kiegészítő folyamatainak leírása mellett tervezni kell az egyes átmeneti folyamatokat is.

Az eddigiekben felvázolt erős matematikai módszer alkalmazása elméleti kutatásokra kiválóan megfelelnek. Ahhoz viszont, hogy a gyakorlatban milyen szinten váltak be ezek az eszközök, az operáció kutatás gyakorlati eredményeit vizsgáltam meg, azon belül is első sorban a döntést támogató rendszereket. Az alábbiakban ezt foglalom össze.

Az operációkutatás modell módszerei egyszerre mutatják az eszközök bőségét, és - sajnálatosan - a gyakorlatban alkalmazott legegyszerűbb modellek alkalmazhatóságának esetlegességét is. Grayson a „Vezetéstudomány és a gazdasági gyakorlat” c. cikkében ennek okát az erős matematikai modellezésben látja, amely rendkívül idő és adat igényes, nem veszi figyelembe az emberi tényezőket, valamint az egyszerűsítő modellezéssel a probléma már közel sem hasonlít az eredeti megoldandó problémára. Kindler József az alábbiak szerint foglalta össze az erős és gyenge módszerek jellemző tulajdonságát:

Minél általánosabb a módszer, annál gyengébb és fordítva. A megoldás során a pótlólagosan bevont feltételezések növelik a módszer erejét, de csökkentik általánosságát. Statikus állapotban nem generál konfliktust, amely az egyensúlyi viszonyt felborítaná, illetve biztonsági szempontból veszélyeztetést okoz. Ebből adódóan, minden ami e stacioner állapot megbomlásához vezet, a környezeti függvény valamely függetlenváltozójának eredményének kell betudni, ami a biztonsági stratégia tervezésének kérdéskörébe tartozik.

Biztonsági stratégia alatt a célfüggvénynek a környezeti függvény hatására történő reagáló képességet értjük. Ezt matematikailag az alábbi konvolúció írja le:

$$S=C \times K = C1k1+c2k2+....Cmkm$$

ahol $Cmkm = (xm, ym, zm;vm) (am;bm,....km)$ szorzata.

A fentiekből adódik, hogy az **S** biztonsági stratégiai függvény, egy skalár - vektor típusú függvény, melynek iránya és nagysága egyértelműen reprezentálja a definícióban megfogalmazott flexibilitást, illetve reagáló képességet.

Az **S** biztonsági stratégiai függvény ismeretében meg lehet fogalmazni a biztonsági stratégiai tervezést és az azt modellező tervezői függvények típusait.

A biztonsági stratégiai tervezés olyan folyamat, melynek célja, hogy a védelem és biztonság homlokterében lévő piaci stratégiai értéket mindenkor összhangban tartsa környezetével. A stratégiai tervezés felkészíti a mindenkori biztonsági vezetést a környezeti változások kezelésére, és biztosítja a rugalmas reagáló képesség rendelkezésre állását.

Ennek a típusú stratégiai tervezésnek éppen az a célja, hogy a különböző környezeti hatások időbeni változásait, módosulásait megfelelőképpen le lehessen kezelni. Ezért a biztonsági stratégiai tervezés egy tervezési rendszer, melynek felépítését az alábbiak szerint lehet összefoglalni:

Sztohasztikus minden, előre nem számolt és a normális üzemvitelt - biztonsági szempontból veszélyeztető kockázati tényező. Ez tovább osztályozható emberi tevékenységtől függetlenül bekövetkező katasztrófa események halmazára, és a emberi tevékenységből származó kár okozásra. Természetesen ez utóbbi esetben meg kell különböztetni a hanyagságot és a gondatlanságot a tudatosan szervezett egyénileg vagy csoportosan - az ismert valamelyik motivációs tényező hatása alatt - elkövetett a biztonságát veszélyeztető támadásoktól.

E dolgozat homlokterében olyan célfüggvény szerepel, melynek független változói determinisztikusak, időben és matematikailag egzakt módon és értékméréssel leírhatóak.

Az alap függvény az alábbiak szerint írható le:

$$CT(x;y;z;v)= C(x(T);y(T);z(T);v(T))$$

Ahol

x: a telekommunikációs eszközrendszer, mely tartalmazza a kapcsolókat, feldolgozókat, tárolókat és továbbító eszközöket,

y: a telekommunikációs eszközrendszerben forgalmazott adatok, kísérőadatokat és közlemények (megjelenési típusaiktól függetlenül),

z: az x és y független változók életgömbjén keresztül kísérő fő és kiegészítő folyamat leírások összessége.

v: az x; y; és z függetlenváltozók fejlesztési, fenntartási, üzemeltetési költség tényezőinek összessége.

A célfüggvény függetlenváltozói biztonsági szempontból potenciális védelemre szoruló tényezők. A célfüggvényt úgy kell tekinteni, mint egy determinisztikus függetlenváltozók által leírt, kockázatokat nem tartalmazó stacioner függvény. Habár kitűnik, hogy a függetlenváltozók között kölcsönhatás, korreláció mérhető, ettől a tényről azzal a valósággal nem sértő egyszerűsítéssel eltekintünk, hogy a közöttük lévő viszony determinisztikus.

A biztonsági stratégiai menedzsment interdiszciplináris, tudomány közti vizsgálatot vállal fel. Ezért nem célja a műszaki - technikai részletekbe elmélyedni. Ugyanakkor a távközlés és az informatika integrációs viszonyrendszerének alapos elemzése megköveteli a két tudományág komplex módszerekkel való bemutatását. A vizsgálat során folyamatosan figyelembe kell tartani, hogy az említett tudományágak önálló fejlődése mellett kölcsönös viszonyban állnak egymással, melyek egy háromdimenziós koordináta rendszerben a hírközlés, az informatika szoros egységet képez a szervezési és vezetési tudományokkal. Ebből az aspektusból vizsgálva mindhárom tudományágról kijelenthető, hogy a legdinamikusabban fejlődtek az elmúlt évszázadban, és ez a folyamat a jövőben is folytatódik. Eredményeik külön-külön is megjelennek mind a polgári szférában, mind a nemzetvédelmi és nemzetbiztonsági feladatok körében.

Ugyanakkor figyelembe kell azt is tartani, hogy a hírközlő és számítástechnikai rendszerek erős integrációt mutatnak. Ebből eredően a védelmi és biztonsági feladatrendszer is rugalmas alkalmazkodást igényel. Ebből az aspektusból tekintve viszont a vizsgálati panel célfüggvényei, illetve azok elemei független változói az alábbiak szerint alakulnak:

$$C(x;y;z;v) \quad K(a; b; \dots k;) \quad \longleftrightarrow$$

Ahol: C a célfüggvény
 $x, y, z, v,$ a célfüggvény független változói,
K a környezetet leíró függvény,
 $a, b, \dots k$ a környezet független változói,

Tervezési rendszer típusai és jellemzői

Statikus tervezés (keret tervezés)

- Hosszabb időre vonatkozó (kb.3 -7 év),
- Főbb nemzeti stratégiai elveket és védelmi objektumokat tartalmaz,
- A tervezés során tetszőlegesen alkalmazhatja a már bevált tervezési modelleket.

Dinamikus tervezés (gördülő terve

- A gördülő tervezés lényege, hogy mindig képes a rövid lefutású, de fenyegetettséget hordó környezeti tényezőket elhárítani és a módosításokat végrehajtani.
- A gördülő tervezés modellje, nyitott bemeneti modell. A környezeti változások paraméter változásaihoz, tetszőleges célfüggvény paraméter változás rendelhető, amely így rugalmas döntés támogató eszközt generál.

Statikus és dinamikus tervezés hatásmechanizmusa

- A dinamikus tervezés szükség esetén akár a statikus tervezési tényezőket is korrigálhatja.
- Az információigény növekedésével azonosan arányban nő a modell módszer erőssége.
- Ha a probléma pontatlanul, homályosan kerül megfogalmazásra, akkor az erős matematikai módszereket nem lehet alkalmazni.

Összességében tehát megállapítható, hogy a problémák megoldásának klasszikus tudományos eszménye az erős módszerek használata, de ugyanakkor tudomásul kell venni, hogy a az erős módszerek használatában korlátozva vagyunk.

Az operáció kutatási modellek fejlődése során az erős, matematikai módszerek és a heurisztikusabb gyenge modellek közötti polarizációt éppen a tudományos technikai fejlődéssel felmerülő bonyolult problémák kezelése oldották fel azáltal, hogy a heurisztikusabb módszereket nem lehet teljes egészében kiküszöbölni a probléma megoldások folyamatából. Ennek konkrét megjele-
nése volt a szimulációs modellezési módszerek kifejlesztése. Ezzel kapcsolatban pedig szükségképpen felmerült a probléma feltárás és megoldás folyamatának tisztázására irányuló kutatómunka. Számos tudományos kutató munka (Potya, Beveridge) kimutatta, hogy a heurisztikus módszerek és az erősebb matematikai módszerek, egymást kiegészítő funkcióval rendelkeznek. Erre mutat példát az a Dr. Kindler J. - Dr. Papp O. által kidolgozott, a tudományos életben KIPA módszerként ismertté vált elemző technika.

Dr. Haig Zsolt mk. alezredes

Információs támadás és hatásai

Bevezetés

A történelem során az egymással szembenálló felek mindig is folytattak szándékos és tudatos célzatú információs tevékenységeket. Ez alatt a régebbi korokban elsősorban a hírszerzést (kémkedést), félrevezetést, propaganda- és nyilatkozatháborút és egyéb hasonló elnevezésekkel említett információs tevékenységeket értettek. Mindezek azonban bármilyen tudatosak is voltak, nem képeztek egy olyan egységes, célzott és határozott struktúrába foglalt információs tevékenységi rendszert, mint amit ma az információs társadalomban gyűjtőfogalommal információs hadviselésnek, vagy katonai terminológiában (NATO) információs műveleteknek nevezünk.

Az információs műveletek – mint összetett információs tevékenységek – az információ szerepének társadalmi felértékelődésével és az információs ipari termelési világkorszak, valamint az információs társadalom kibontakozásával összefüggésben tudatosan jelennek meg.

Az ellenfél gazdasági hitelrontását, politikai megbízhatóságának kétségbevonását a mindennapi életben gyakran barátságtalan lépésnek lehet tekinteni. Az ilyen információs tevékenységek, lépések azonban nem mindig vezetnek kifejezett információs műveletekhez. Ilyen helyzetekből még vissza lehet térni a felek közötti kapcsolatokban általánosan elfogadott normális viszonyokhoz és dinamikus egyensúlyhoz. Ugyanakkor fontos jelzés és üzenet értékű jelentéstartalma van annak, ha a közös kapcsolatokat érintő, dinamikus egyensúly fenntartására irányuló törekvésekben hirtelen, heves és jelentős változások következnek be. Ezek hatására olyan további információs tevékenységek kezdődhetnek, amelyek már az információs műveletek kelléktárába tartoznak.

Békeidőszakban, feszültség- vagy válsághelyzetben a nemzetgazdaság, illetve az alapvető polgári információs infrastruktúrák ellen végrehajtott nagyméretű, korlátozó vagy pusztító hatású információs támadások adott esetben egy háború bevezető szakaszát is jelenthetik. Ezért az információs rendszerek és infrastruktúrák védelme alapvetően fontos biztonságpolitikai tényezővé vált.

Az információs műveletek új fajtájú hadviselési forma, amely a 21. század első évtizedeiben bontakozik ki teljes terjedelmében, amikor az iparilag fejlett országok fokozatosan átlépnek az információs korszakba és az országok életében a távközlési és információtechnikai eszközök, rendszerek és hálózatok meghatározó szerepet fognak betölteni. Az információs társadalmak sebezhetősége éppen az információtechnika és az információs infrastruktúra révén rendkívüli mértékben megnövekszik. Viszonylag kis költségráfordítással olyan információs támadó fegyvereket és fegyverrendszereket lehet előállítani, amelyek különböző mértékű, hatású és időtartamú pusztításokat vagy korlátozóso-

kat képesek előidézni. Ezeknek a veszélyeknek felismerése és a megfelelő ellenrendszabályok kialakítása, minden ország jól felfogott, saját érdeke.

1. Ráhatás a vezetési folyamatra

Az információs fölény és uralom megszerzéséért folytatott erőfeszítések elmélete – többek között – a kommunikáció elméletén (a rendszerek közötti kapcsolatok és viszonyok elmélete), valamint a káoszelméleten alapul. A kommunikáció elmélet szerint a társadalmi szervezetek között alapvetően kétféle kapcsolati csatornán áramlik az anyag, energia és az információ, úgymint:

- közlekedési, szállítási, logisztikai csatornákon valamint
- távközlési és információs hírcsatornákon, melyek fenntartják a szervezetek belső integritását.

Az információs fölény megszerzéséért folytatott erőfeszítések lényege abban áll, hogy amennyiben a szervezetek, rendszerek közötti információs csatornákat elvágják, elszigetelik, működésüket bénítják, vagy korlátozzák, akkor bekövetkezik a rendszerek önzáródási effektusa, amelyben az érintett szervezet, vagy rendszer csak saját információs és egyéb erőforrásaira tud támaszkodni. A saját erőforrások intenzív belső felhasználásának törvényszerű eredménye, hogy az érintett rendszerben beindul a káosztörvény érvényesülése, vagyis a szervezett rendből, az irányíthatóságból és vezethetőségből öntörvényűen kialakul a szervezatlenség, irányíthatatlanság, vezethetatlenség állapota. Az információáramlástól megfosztott katonai szervezeteknél is érvényesek ezek a hatások, vagyis megtörténik a szervezeti, rendszeri és tevékenységi összeomlás, bekövetkezik a „fekete lyuk effektus”. Az információs támadás esetében a szembenálló fél oldalán pontosan ilyen helyzet előidézése a cél. [1; 2]

Az információs fölény a győzelemhez nélkülözhetetlen, de annak nem egyedüli feltétele. Az információs fölény e fokozatai, összehatásukban elvezetnek a szembenálló fél feletti tartós és szilárd vezetési fölény kialakulásához, amely a siker egyik fontos záloga.

A vezetési fölény egyrészt a szembenálló felek vezetési folyamatai között olyan minőségi különbséget jelent, amikor az egyik fél tevékenységét meghatározó parancsok, utasítások tartalma és időbelisége lényegesen jobban tükrözi a kialakult helyzetet, és az ahhoz alkalmazkodó célszerű cselekvésmódot, mint a másiké. Másrészt azt az állapotot fejezi ki, amikor ugyanezen fél végrehajtó állományának eltökéltsége a parancsok teljesítésére azonos vagy nagyobb, mint a másik felé.

A vezetési fölény kivívása a saját információfeldolgozási és kommunikációs rendszer hatékony alkalmazására, az információk célirányos és szakszerű felhasználására, a teljes vezetési rendszer optimális működtetésére irányul, amely összességében két fő tényező függvénye, úgymint:

- az információs fölény és uralom kivívása, és
- a saját vezetési és információs rendszer által biztosított lehetőségek hatékony felhasználása, a döntési ciklus lerövidítése, a döntések minőségének fokozása, valamint a kapcsolódó parancsok hatékony kidolgozása és továbbítása érdekében. [1]

Ennek következtében a saját vezetési tevékenységünk időtartama a szembenálló fél vezetési tevékenységének időtartamán belülre kerül, gyorsabbak vagyunk, gyorsabban észlelünk, döntünk és intézkedünk, mint a szembenálló fél.

A saját vezetési képességeink maximális kihasználása, és a szembenálló fél vezetési képességeinek részleges vagy teljes akadályozása jelentős erősösztető tényező, amely a harcfelelőlt végrehajtásában nyilvánul meg. A saját erők pontos és hiteles információkon alapuló elhatározás alapján végzik feladataikat. Az előljáró folyamatosan kapcsolatban van az alárendeltjeivel, akik a valós helyzetre reagáló feladataikat szervezeten képesek végrehajtani.

Ezzel szemben a szembenálló fél információhiányban szenved, a parancsok döntései pontatlan és csak valószínűsíthető információkon alapulnak. Az alárendeltjeivel való kapcsolattartás bizonytalan vagy lehetetlen, aminek következtében parancsait, intézkedéseit nem tudja lejuttatni a végrehajtói szintre, illetve azok képtelenek helyzetükről tájékoztatni az előljárót. Ennek eredményeként a feladat végrehajtása irányítatlan, kaotikus. A szembenálló fél csapatai nem képesek a valós helyzetre reagáló szervezett erőfeszítésre.

2. Új típusú hadviselési elvek

A vezetési időciklus csökkentésére való törekvés szoros kapcsolatban van az információs fölény és a vezetési fölény kialakításának képességével. Az információs fölény és a vezetési fölény elérése és megtartása merőben új típusú hadviselési elvek, formák, módok alkalmazását teszik szükségessé. Ezek az új elvek gyökeresen más aspektusból közelítik meg a siker eléréséhez vezető utat. A pusztítás, rombolás, emberi élet kioltása helyett a hatékonyság, az élőerő megóvása, a manipuláció, és a vezethetlenségi állapot előidézése a cél. Ez azt jelenti, hogy az információalapú hadviselési módok, a végső sikert jelentősen befolyásoló szerepet kapnak.

E hadviselési módok az információt egyrészt a vezetési folyamatban és a fegyverirányításban használják fel, mint vezetési eszközt, másrészt, pedig mint támadó és védelmi fegyvert alkalmaznak. Ezek az említett új típusú hadviselési elméletek és eljárások a hatásalapú műveletek, a hálózatközpontú hadviselés és az információs műveletek köré csoportosíthatók, és amelyek új jelenséggé jelennek meg a hadviselés területén. Eme új tevékenységekben – a tudományos és hadiipari komplexumok fejlesztő képességének rendkívül gyors ütemű megnövekedése következtében – új eszközök, szervezési elvek, hadviselési módok stb. kerülnek bevezetésre. Pusztán megjelenésükkel és az újdonság ere-

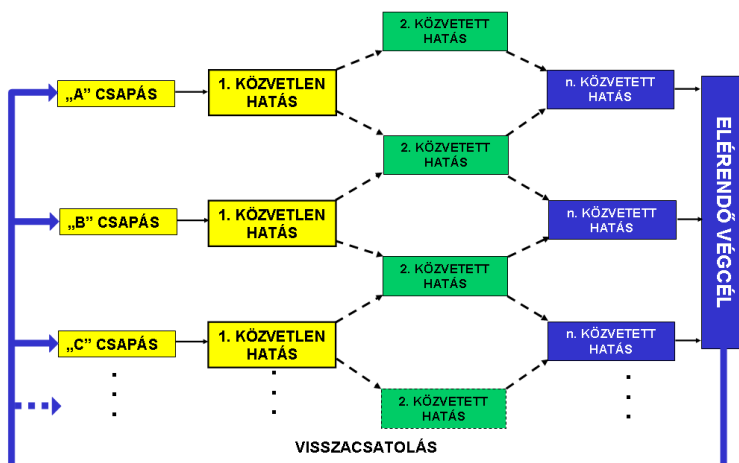
jénél fogva komoly „meglepetési fölényt” biztosíthatnak, amelyekre – képesség hiányában – a potenciális ellenfelek nyilvánvalóan nem tudnak felkészülni. Az információs műveletek elmélete szerint, egy társadalomban első- és másodfokú társadalmi–technikai civilizációs fejlettségi rend működhet. A fejlett társadalmi rendszerek jogi és erkölcsi törvényekkel, szabályzókkal, szabványokkal irányítottan léteznek és működnek. Ezek a társadalmak – a magas fokú szervezethez – erősen szabályozott társadalmi rendhez tartoznak, amelyet második fokozatú fejlettségi szintnek nevezünk. Amennyiben ez a magas fokú szervezethez – valamilyen külső–belső negatív társadalmi–természeti oknál fogva – megszűnik, vagyis a fejlett törvények és szabályzók már nem képesek működni és hatni, akkor az érintett szervezeteknél és technikai rendszereknél bekövetkezik a dereguláció, egy társadalmi–technikai visszaesés az első fokozatú civilizációs szervezethez, ahol a természet törvényei objektív módon – a kaos törvénye szerint – hatnak. Az információs műveletek során a társadalom alapvető érdeke saját oldalán a második fokozatú civilizációs rend fenntartása és az ellenfélnél az első fokozatú civilizációs rend ideiglenes kialakítása, vagyis irányíthatatlan helyzet, sajátos kaosrend előidézése. [5]

Az információs támadás céljai között szerepel a szembenálló fél rendszereinek, hálózatainak, szervezeteinek megfosztása attól a lehetőségtől és képességtől, hogy külső anyagi utánpótlást, új fegyvereket, energiát vagy vezetési információt kapjanak. További célok közé tartozik annak megakadályozása, hogy az ellenfél védelmi rendszerei egymás között ilyen típusú éltető erőforrásokat, (anyagot, energiát, információt) és a túlélést biztosító logisztikai szállítmányokat cserélhessenek. Ez történhet a védelmi és logisztikai kommunikációs folyamatok teljes megszakításával, működésük tartós korlátozásával, vagy ideiglenes kikapcsolásával, zavarásával. Más szóval a szembenálló fél védelmi rendszereinek a magasabb második fokozatú fejlettségi rendből az alacsonyabb első fokozatú fejlettségi rend szintjére történő visszavetésével. Ez a törekvés azt is magában foglalja, hogy megakadályozzák az anyaggal, energiával, információval történő segítségnyújtást.

A fenti célok elérését biztosító információs támadásokat közvetlenül – egyes kijelölt célpontokra koncentráló direkt támadási módszerrel – vagy közvetett módon – a mélységben lévő kritikus célpontok, hálózatok, rendszerek elleni indirekt támadással – lehet végrehajtani. Nem ritka a közvetlen és közvetett támadási eljárás, módszer kombinálása. Az információs támadások a célpontok szövevényes összefüggése, több szintű rétegződése és mátrix jellegű hálózatos kapcsolódása következtében gyakran nem egyes célpontok ellen irányulnak. Ehelyett inkább az egész rendszert érintő és káros hatást kifejtő, háborús teljesítményt csökkentő, úgynevezett degradáló, deregulációs hatás elérését célzó eredményre törekszik a hatásalapú műveletek keretében.

A hatásalapú műveletekben a korábbi felfogáshoz képest az a lényeges változás, hogy 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. Ez az új hadművelleti felfogás a holisztikus elvű személet alkalmazását igényli, amelynek lényege, hogy minden mindennel összefügg, és minden elem hatással van a többi elemre is.

A közvetlen első hatás és közvetett hatások elvének mélyreható tudományos vizsgálata feltárta, hogy egy rendszer belső elemeire mért pusztító, vagy korlátozó jellegű csapás mind a rendszeren belül, mind pedig a rendszerek közötti kapcsolatokban – a földrengéshez hasonlóan – másod, harmad és n-edik típusú és erősségű hatásokat vált ki (1. ábra). E műveletek végrehajtása során tehát az egyensúly fenntartásában kulcsszerepet játszó pilléreket keresik, és támadják. A hatásalapú műveletek tervezésekor mindig az elérendő – kívánt – végállapotból indulnak ki, és ehhez mérten tervezik a különböző kinetikus és nem kinetikus energia elven működő csapásokat, vagy ráhatásokat. [3]



1. ábra: A hatásalapú műveletek hatásláncolata

3. Információs támadási formák és hatások

Az információs műveletek céljai elérése érdekében fizikai-, információs- és tudati – az emberi felfogóképeség és megértés – dimenzióiban fejti ki hatását.

A fizikai dimenzióban folytatott információs műveleti tevékenységek a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni ún. „kemény típusú” („HARD KILL”) támadásokat, illetve azok fizikai védelmét jelentik.

Az információs dimenzióban folytatott információs műveleti tevékenységek a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció, stb. többnyire elektronikus úton való „lágy típusú” („SOFT KILL”) támadását jelenti annak érdekében, hogy a célpontokra való közvetlen pusztító, romboló fizikai ráhatás nélkül közvetlenül befolyásoljuk azokat. Másik oldalról ide tartozik a szembenálló fél saját információs folyamatainkra irányuló hasonló támadásának megakadályozása is.

A tudati dimenzióban megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást – észlelést, érzékelést, értelmezést, véleményt, vélekedést – veszik célba valós, csúsztatott vagy hamis üzenetekkel, amelyeket többnyire elektronikus és nyomtatott médián keresztül vagy közvetlen beszéd formájában továbbítanak.

Az információs műveletek támadó és védelmi képességekkel biztosítják az információs fölény elérését és fenntartását. A védelmi képességek a saját információs rendszerek működését, információs lehetőségek kihasználását biztosítják, a támadó képességek pedig a szembenálló fél információs rendszerei ellen irányulnak.

Az információs támadás típusai, képességei köz soroljuk az információs infrastruktúrák fizikai pusztítását, a megtévesztést, az elektronikai hadviselést, a pszichológiai műveleteket, a számítógép-hálózati hadviselést és a felderítést. Az információs támadás felsorolt képességei a szembenálló fél, irányában számos hatástényezőn keresztül érik el célkitűzéseiket. Ezen hatástényezőket és az információs támadás képességei közötti összefüggéseket a 1. táblázat szemlélteti.

A katonai műveletek során, a fenti tevékenységeken belül ún. „halálos és nem halálos fegyvereket” alkalmazhatunk a háborútól való elrettentés vagy a béke-teremtés céljára, illetve a meghatározott háborús feladatok célkitűzéseinek elérése érdekében. Az információs támadás során szintén alkalmazzuk mindkét eszközfajtát, azonban e műveletekben többségében a nem halálos technikákkal, az ún. „SOFT KILL” eszközökkel is jelentős sikereket lehet elérni. Az információs támadás folytatásakor a nem halálos eszközökkel úgy tudjuk befolyásolni a kialakult helyzetet, hogy adott esetben a fegyveres konfliktus elkerülhetővé válik. Ebben jelentős szerepe lehet a média nagyfokú felhasználásának, az ún. „CNN hatás” kihasználásának, amikor a médián keresztül olyan

üzeneteket tudunk közvetíteni mind a saját erők irányába, mind pedig a szembenálló fél felé, ami a válság további eszkalálódását megakadályozhatja.

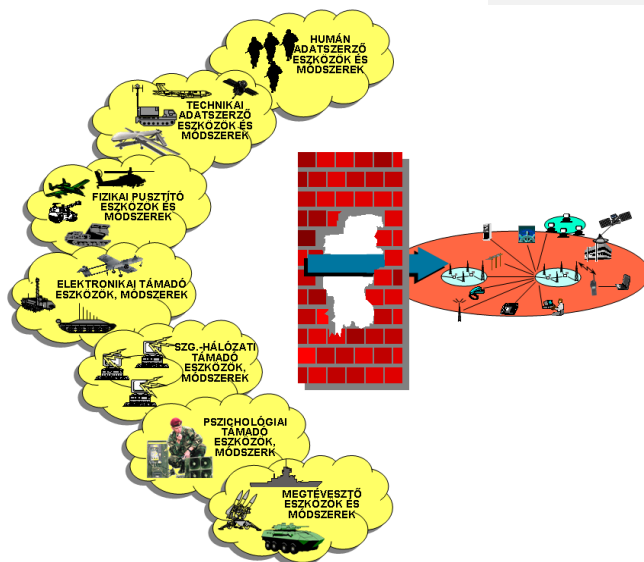
1. táblázat: Az információs támadás képesség és hatás mátrixa

Képesség Hatás	Pusztítás	Megtévesztés	Elektronikai hadviselés	Pszichológiai műveletek	Szg.-hálózati hadviselés	Felderítés
Meggyőző						
Leront						
Megfoszt						
Pusztít						
Csökkent						
Megszakít, meg-						
Befolyásol						
Tájékoztat						
Megelőz, meghiusít						
Félrevezet, megté-						
Megvéd, oltalmaz						
Megtagad						
Semlegesít, hatástala-						
Formál, alakít						
Hasznosít, kihasznál						
Felfed, láthatóvá tesz						

Az információs támadás az információhoz való hozzáférés megnehezítésével, és a vezetési rendszerek működésének befolyásolásával megakadályozza a szembenálló fél vezetési lehetőségeinek hatékony kihasználását. Az információs támadáson belül különböző lehetőségek vannak a szembenálló fél információs rendszereinek működésének akadályozására. Ezek a következők:

- az információhoz való hozzáférés lehetetlenné tétele az adatszerzés akadályozásával;
- a másik fél vezetőinek, parancsnokainak befolyásolása, döntési képességeinek manipulálásával;
- a szembenálló fél információs műveleteinek akadályozása az információs rendszerek szelektív megzavarásával;

- a számítógépes hálózatok működésének befolyásolása, akadályozása különböző rosszindulatú szoftverek bejuttatásával;
- a szembenálló fél információs képességeinek hatástalanítása a különböző vezetési objektumok fizikai pusztításával. (2. ábra)



2. ábra: Támadó információs műveletek eszközei és eljárásai

Az információs támadás különböző képességei arra irányulnak, hogy speciális célok érdekében vagy speciális fenyegetésekre válaszul, hatást gyakoroljanak a potenciális szembenálló fél információira, információalapú folyamataira, információs rendszereire békeidőben, válság vagy konfliktus idején egyaránt. Információs támadásokkal képesek vagyunk lelassítani, és megzavarni a másik fél feladatai tervszerű végrehajtásának ütemét, akadályozni az erő kifejlesztés összpontosítását, valamint befolyásolni a kialakult helyzet értékelését.

Az információs támadásoknak kettős funkciójuk van. Egyrészt minden lehetséges eszközzel **elfogni, felfedni** a másik fél információit, aminek következtében az információ bizalmassága sérül. Másrészt **befolyásolni, tönkretenni** a szembenálló fél információit, amelynek eredményeként nő az adatok és információk sérülékenysége, a különböző szolgáltatásokhoz való hozzáférés pedig csökken. E kettős funkciót a fizikai-, információs- és a tudati- dimenzióban egyaránt, egymással összehangoltan kell érvényre juttatni. (2. táblázat)

2. táblázat: Az információs támadás hatása és támadási dimenziói [4]

Funkció:	ELFOGÁS, FELFEDÉS		BEFOLYÁSOLÁS, TÖNKRETÉTEL					
Biztonsági jellemző:	Bizalmas-ság sérül		Adatok sérülékenysége nő Szolgáltatások elérhetősége csökken					
Forma:	Közvetett	KÖZVETLEN	Közvetett			Közvetlen		
Támadó tevékenység: Támadási szint:	Információ források felderítése		Megtévesztés	Zavarás	Pusztítás	Megtévesztés	Zavarás	Pusztítás
Tudati dimenzió	Viselkedési formák, befolyásolhatóság megfigyelésével következtetés a megértési és döntési folyamataitokra	Párbeszéd, döntési folyamatok megfigyelése HUMINT mód-szerekkel	Döntéshozatal, megértési folyamat befolyásolása PSYOPS tevékenységekkel (szórólapok, média, Internet alkalmazása)			Titkos műveletekkel beszivárgás a célközönség közé és ott a megértési folyamatot befolyásoló témák terjesztése		

Információs dimenzió	Üzenetek, közlemények passzív módszerekkel való lehallgatása Hálózati topológia kívülről való feltérképezése Titkosítás megfejtés, dekódolás	Elektronikai felderítő szenzorok alkalmazása Számitógép hálózatok adataihoz való rejtett hozzáférés Trójai programok alkalmazása Jelzőszólopók telepítése	Megtévesztő e-mail üzenet továbbítása Megtévesztő hálózati tevékenységek folytatása	Hálózatok adatokkal való mesterséges túlterhelése (FLOOD ATTACK), ezáltal a hálózati hozzáférés akadályozása Szenzor adatok bejuttatása, melyek megzavarják az irányítási folyamatokat (pl. légvédelem) Nyílt forrású információkkal a figyelem elterelése	Trójai programok bejuttatása megtevesztő tevékenység útján Működő programok -kal (virulens ágens) adatok módosítása	Rosszindulatú szoftverekkel, programokkal (férgek, vírusok stb.) hálózati szolgáltatásokhoz való hozzáférés megakadályozása, adatok, adatbázisok tönkretétele
Fizikai dimenzió	Monitorok VAN ECK féle kisugárzásának felfedése Vezetékes vonalak induktív módon való lehallgatása Párhuzamos kutatása	Információs eszközök, titkosító kulcsok, fizikai kulcsok, adattároló hordozók ellopása	Titkos információhoz való hozzáférés a felhasználó félrevezetésével (SOCIAL ENGINEERING)	Bomlasztó tevékenységek előidézése a felhasználók félrevezetésével	Fizikai biztonságot feltörve, titkos adatokhoz való hozzáférés	Információs infrastruktúrák fizikai rombolása Információs rendszerek és azok elemeinek elektronikus támadása

Az információs támadás **közvetlen** és **közvetett** formában valósulhat meg. A **közvetlen információs támadás** – más néven belső vagy behatoló jellegű támadás – során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a kommunikációs rendszerekbe és számítógép-hálózatokba, hozzáfér különböző adatbázisokhoz stb. és ezáltal számára hasznosítható **információkhoz jut**. Másrészt zavaró jelekkel, megtevesztő információkkal, rosszindulatú szoftverek bejuttatásával **tönkreteszi, módosítja, törli** stb. a szembenálló fél számára fontos információkat.

A **közvetett információs támadás** – más néven külső vagy szenzor alapú támadás – során a támadó fél hozzáférhetővé teszi a szembenálló fél számára a saját félrevezető információit, ezáltal **megteveszti a szembenálló fél felderítő rendszerét** és így befolyásolja a helyzetértékelését. [4]

Természetesen a közvetlen és közvetett támadást megfelelően összehangolva célszerű alkalmazni, ezáltal is erősítve egymás hatékonyságát. Egy közvetett információs támadással el lehet terelni a felderítő rendszerek figyelmét, így a közvetlen támadás sikeresebben végrehajtható a megcélzott rendszerrel szemben. Ugyanakkor egy közvetlen módon végrehajtott információs támadás arra kényszerítheti a vezetési rendszert, hogy pl. a döntési alternatívák kialakítása-kor, az összadatforrású felderítő rendszer helyett csak egy forrásból származó információkra, pl. csak az optikai felderítésre támaszkodjon. Ez az egyforrású felderítő rendszer pedig a már említett közvetett támadással, pl. makettek alkalmazásával hatékonyan félrevezethető. A felsorolt támadási funkciókat, formákat és konkrét tevékenységeket azok hatása és támadási szintjei szerint a 2. táblázat szemlélteti.

Összegzés, következtetések

Az információs támadás alkalmazásával nagymértékben lehetővé válik a hagyományosnak tekinthető erők és eszközök gazdaságos felhasználását.

Az információs támadás eredményeként a szembenálló fél vezetési, információs rendszereinek működése leromlik, vezetési ciklusuk ideje jelentősen megnövekszik. Ebben a helyzetben a szembenálló fél képtelen megfelelően irányítani alárendeltjeit, pontosan meghatározni számukra a harcfeladatokat, tehát a vezetési folyamatban káosz jelentkezik, bekövetkezik a vezethetatlenség állapota. Így a szembenálló fél tűzeszközeinek alkalmazása kaotikussá válik, esetleg azok a teljes használhatatlanság állapotába kerülnek.

Elemmezve az információs támadás képességeit, ezzel párhuzamosan az ország biztonságát, illetve az arra ható tényezőket, arra a következtetésre jutunk, hogy nem hagyhatjuk figyelmen kívül az információs szférából érkező támadásokat, melyek az ország információs infrastruktúrái ellen irányulnak. Azt is szem előtt kell tartanunk, hogy ezek a támadások – az aszimmetrikus fenyegetéseknek megfelelően – nem csak egy másik ország fegyveres erejétől származhat-

nak, hanem akár egyes személyektől, csoportoktól, vagy különböző terrorista szervezetektől is.

Felhasznált irodalom:

1. Haig, Zsolt–Várhegyi, István: A vezetési hadviselés alapjai. Egyetemi jegyzet, ZMNE Budapest, 2000.
2. Várhegyi István – Makkay Imre: Információs korszak, információs háború, biztonságkultúra. OMIKK, Budapest, 2000.
3. Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.
4. Waltz, Edward: Information Warfare Principles and Operations. Artech House, Inc. Boston, London. 1998. ISBN: 0-89006-511-X.
5. Wheatley, Margaret J.: Vezetés és a modern természettudomány – rendszer a káoszban. SHL Kiadó, Budapest, 2001.

Kassai Károly

Az elektronikus információvédelmi rendszabályok
megalapozásának fontosabb kérdései

Napjainkban nem szükséges indokolni az információk és adatkezelő rendszerek biztonságának fontosságát.

A szövetségi környezethez harmonikusan illeszkedő korszerű elektronikus adatkezelő képességek védelmi rendszabályainak általános megfogalmazásához szükség van az igények áttekintésére, majd ehhez kapcsolódóan az átfogó követelmények meghatározására.

1. Szervezeti elvárások, általános követelmények

A hálózat centrikus hadviselés elméletét megalapozó cikkben¹⁸ Arthur K. Cebrowski és John J. Garstka szerint a hálózat centrikus hadviselés (network centric warfar; NCW) hozzájárul a *vezetés felgyorsulásához*, és lehetővé teszi az erők *teljes mélységű szervezését és összehangolását*. Elemei a *nagyteljesítményű hálózat* a szükséges információs források és fegyverek eléréséhez, a *precíziós csapások és nagysebességű manőverek*, az értéknövelt információs folyamatokban megnyilvánuló *vezetési és irányítási rendszer (C2)*, valamint az integrált, fegyverirányítással és C2 folyamatokkal összekapcsolt *szenzorhálózatok*.¹⁹ A gyorsabb vezetés alapja az *információs fölény*, az *erők sebességben, precizitásban és reagáló képességben megnyilvánuló hatás alapú alkalmazása*.²⁰

A NATO Stratégiai Vízión (The Military Challenge) helyzetértékelésként megállapítja, hogy a szövetség egy szélesben értelmezett, számtalan tényező által befolyásolt stratégiai környezetben működik (globalizáció, megoldatlan konfliktusok, radikális ideológia, aszimmetrikus kihívások).

¹⁸ A szerzők szerint a hálózat centrikus hadviselés modellje alkalmazásának halasztása magasabb költségeket, a harci erők csökkentett képességét, illetve általánosságban a 2010-es Stratégiai Vízión megvalósulását veszélyezteti.

¹⁹ A hálózatközpontú hadviselés nélkülözhetetlen elemét – a szenzorrácsot – Hóka Miklós mutatta be cikkében. Ennek lényege, hogy a hadműveleti területet teljesen lefedő fizikai vagy virtuális érzékelők megjelennek a terepen, a gépjárműveken, felszerelési tárgyakon és fegyverirányítási rendszereken és már nem csak a környezetről vagy ellenségről gyűjtenek és továbbítanak adatokat.

²⁰ Szép József 2004-ben ehhez hasonlóan mutatta be a hálózat nyújtotta képesség alapelveit (az *információ megosztás, a megosztott helyzetkép, és ezáltal az önszinkronizáció lehetősége*).

A *hatás alapú* (effect based operation; EBO) megközelítés a szövetség katonai és nem katonai erejének összetett, integrált minden vezetési szinten, a konfliktusok teljes skálájánál történő alkalmazása. Ennek érdekében fejleszteni kell a *felderítést*, az *adatok megosztását*, az *előrejelzést*, valamint robosztus és rugalmas híradó és informatikai rendszeren alapuló *hálózat alapú képességeket* kell kialakítani a *hadműveleti környezet teljes körű ismerete* és a megelőző jellegű beavatkozás érdekében.

A hatás alapú műveletek az erők és képességek széleskörű integrációját kívánják a *döntési fölény* (Decision Superiority), a *koherens hatások* (Coherent Effects) és az *összhaderőnemi telepíthető és fenntartható erők* (Joint Deployment and Sustainment) érdekében.²¹ A *döntési fölény* kritikusan függ az *információs fölény*²² kialakításától és fenntartásától, valamint a műveletek minden fázisában a *helyzetismeretre vonatkozó adatok megosztásától*. A döntési fölény alapja a hadműveleti helyzet ellenséghez képest jobb megértése, és a *döntési ciklus napokban mért hosszának órákra, percekre történő csökkenése*. Az új vezetési és irányítási rendszereknek lehetővé kell tennie az információs fölény átalakítását *akcióképes ismeretté*, ez által támogatva a gyorsabb tervezést, a jobb döntéseket és a döntő hatások elérését.

Ebben a környezetben kulcsfontosságú tényező az *interoperabilitás*²³ és az *összekapcsolhatóság*.

Koherens hatás akkor érhető el, ha a *katonai erők integrálják képességeiket* a szövetség minden eszközével és erőforrásával, és a hadműveleti

²¹ NATO Strategic Vision 5, 6, 7, 8, 28. p.

²² A NATO ACT megfogalmazása szerint az információs fölény célja olyan környezet biztosítása, ahol a rendelkezésre álló információk minősége és mennyisége jelentős előnyt biztosít a menedzselt, elosztott és együttműködő folyamatokra, eszközre támaszkodva (Information Superiority & NATO Network-Enabled Capability (Fact sheet); www.act.nato.int).

Munk Sándor 2001-ben ismertette az információ különböző „szintjeit” (nyers adat, feldolgozott adat (információ), az ez után értelmezéssel kialakuló ismeret valamint ez után a megítélésen alapuló megértés). Ezen keresztül látható, hogy az információs fölény nem önmagában nem elégséges a döntési fölény kialakulásához, mert ahhoz a *kialakult tudásszinttel támogatott döntésre van szükség*.

²³ Munk Sándor interoperabilitás területén végzett vizsgálata megállapította, hogy a rendeltetés-szerű működés és a feladatok eredményes ellátása érdekében az informatikai interoperabilitás területén szükség van a *célok, alapelvek és tevékenységi irányok* meghatározására. Ennek elmaradása esetén olyan rendszerek/eszközök kialakítása, fejlesztése, beszerzése történhet meg, amelyek *nem képesek a katonai műveletek során a szükséges mértékű együttműködésre*.

területen a katonai műveletek és nemzetközi, nemzeti, valamint nem kormányzati szereplők erőfeszítései szorosan összehangoltak.

Az összhaderőnemi telepíthetőség és fenntarthatóság lehetővé teszi a szövetség folyamatos, elosztott, vagy nem folyamatos műveletekre szabott erőinek időbeni alkalmazását, és a műveletek támogatását bárhol, ahol arra szükség van.²⁴

A stratégiai vízióban a döntési fölény – és a másik két cél – támogatására szolgáló hálózat alapú képesség (network enabled capability; NEC) kialakítása érdekében több tagállam összefogásával 2004-ben kezdődött kutatás, melynek eredménye a NATO NEC (NNEC) megvalósíthatósági tanulmány (NNEC Feasibility Study), ami a hálózatosított információs infrastruktúrára vonatkozó szükségletet a következőkben határozza meg:

a hálózati képességek kiterjesztése („bárhol ahol szükséges, bármikor, amikor szükséges”);

a kisebb, moduláris rendszerű, többnemzetiségű erők támogatása (új típusú információ megosztási és biztonsági követelmények, valamint interoperabilitásra vonatkozó elvek szükségessége);

a nemzeti elemek rotációjának támogatása, valamint az interoperabilitási követelményeket nem teljesítő nem NATO nemzetek támogatása az NRF kötelékeken belül.²⁵

A NATO tanulmány integrálja a brit hasonló témájú tanulmány eredményeit, melyben világosabban megmutatkozik a hálózat alapú képesség három egymással átfedésben és szoros összefüggésben lévő dimenziója: a *hálózatok* (hozzáférés, rugalmasság, menedzsment és technikai interoperabilitás), az *információ* (előállítás, hozzáférhetőség, a védelem és a biztonság szükséges szintjének szavatolása) és az *emberek* (egyéni és csoportos oktatás és képzés, team típusú képzés, interoperabilitás).²⁶

²⁴ NATO Strategic Vision 28, 30, 32. p.

Haig Zsolt -Várszegi István 2005-ben ehhez hasonlóan bemutatta, hogy a katonai információ rendszerek feladata a *döntési ciklus minél hatékonyabb támogatása* (a környezetről, ellenségről szóló adatgyűjtés, feldolgozás, értékelés, a saját erők állapotának nyilvántartása, a lehetőségek vizsgálata, a cselekvési változatok kialakítása, a döntéstámogatás, valamint a változó helyzet által generált újabb és újabb adatgyűjtési és feldolgozási ciklusok kiszolgálása), és az ezzel járó *erősokszorozó hatás* elérése.

²⁵ NNEC FS 1. 2. 4. p.

²⁶ NEC, JSP 777 edition 1; ww.mod.uk..

*Az információ biztonság szavatolására irányuló mechanizmusok az információs infrastruktúra minden területére beépülve, egymással együttműködve fejtik ki hatásukat. Biztosítják, hogy a megfelelő személyektől, a kellő időben rendelkezésre bocsátott információ valóban megbízható (trusted) legyen, így megvalósul az elterjedőben lévő információ megosztásra vonatkozó elv (duty to share), kiegészítve a szükséges, hogy tudja (need to know) elvvel. A megosztásra vonatkozó elv alkalmazása lehetővé teszi, hogy a rendszerek tervezésekor, alkalmazásakor a politikák, eljárások tartalmazzák az ehhez szükséges képességeket; ugyanakkor a védelmi rendszabályok alkalmazása biztosítja, hogy csak a megfelelően felhatalmazott személyek férhessenek hozzá az adatokhoz.*²⁷

A megvalósíthatósági tanulmány megjelenése után kialakult a hálózat alapú képesség víziója és koncepciója (NNEC Vision and Concept), mely a képesség fontosabb jellemzőjeként három területet azonosít:

A tartalomszolgáltatás (informational content) fejlesztése, valamint a kulturális és humán tényezők összehangolása.

Azonos interfészek, szolgáltatások kifejlesztése és adoptálása. Az új követelményeknek megfelelő könnyebb és gyorsabb alkalmazhatóság, valamint a költségtakarékosság érdekében a szervezeti elemek és képességek moduláris, blokk-rendszerű tervezése.

Az információ megosztásra vonatkozó képességek fejlesztése, valamint a szolgáltatások bizalmassági szintjének emelése az információ biztonság szavatolásának és a biztonsági politikák továbbfejlesztése segítségével. A határokon átnyúló, egyre erősödő információ csere területén a „duty to share” elv alkalmazása.²⁸

Az NNEC koncepció *a hálózatok, szolgáltatások, és folyamatok föderációjának elméletére* támaszkodik, mely szerint a független alrendszerek, képességek központi menedzseléssel stratégiai szinttől harcászati szintig egyaránt elérhetővé válnak a *hálózati és információs infrastruktúrákon*

²⁷ NNEC FS 6. 1. 4. Az említett általános követelmények mellett a vízió konkrét elemeket is tartalmaz, mely szerint az *IP rejtjelzés*, és a *kulcs menedzsment infrastruktúra* alapvető követelmény a megfelelő védelemmel ellátott kommunikáció érdekében. Az egyik legnagyobb kihívás a szövetség szintű telepíthetőség.

²⁸ NNEC VC 8. p.

(networking and information infrastructures; NII) keresztül.²⁹ A koncepció megvalósítása *kognitív* és *technikai* területekre bontható.³⁰

A *kognitív képességek* feladata a rendelkezésre álló információk átalakítása felhasználható tudássá. Ennek részei az *együttműködés* (az információ tulajdonos szervezetek, alkalmazások között), az *információ megosztás* (az elkülönült adatok összeillesztése a szükséges háttér kialakítása érdekében), az *információ feldolgozása* (adattűzés, melynek eredményeképpen az adott helyen, a szükséges tartalom jelenik meg, ahol az alkalmazást megfelelő képzési és gyakorlási háttér támogatja). Az említettek hatékony *információs erőforrás menedzsment*, valamint az információkat eredményesen alkalmazó *szervezeti elemek és műveletek* kialakításával válnak működőképes egésszé.

A *technikai terület* feladata a meglévő képességek hálózat alapú képességgé történő fejlesztése. Ennek részei a hálózat alapú képesség *architektúrájának kialakítása*, a *szolgáltatás alapú megközelítés* (a szükséges szolgáltatások több üzemeltetési környezetben történő alkalmazhatósága), a *moduláris felépítés* (gyors átkonfigurálási lehetőségek, az elemek rugalmas korszerűsítése), az *információ biztonság szintjének szavatolása* (fejlett szintű rejtjelzés és kulcs menedzsment infrastruktúra, objektumok címkézése, a kockázatelemzés hangsúlyosabb alkalmazása, szabványok alkalmazása az információvédelmi rendszabályok területén, interoperabilitás) és a *szolgáltatás menedzsment*.

A katonai dimenzióhoz hasonló fejlesztési irányokat, követelményeket tartalmaz az EU stratégiai keretrendszer is. A kitűzött „egységes európai információs tér” tértől és időtől függetlenül elérhető gazdag médiatartalmat és új, változatos formátumokat jelent, ami a távközlési hálózatok, a médiumok, a tartalom, a szolgáltatások és az eszközök *digitális konvergenciájának eredménye*. A kialakítás során a sebesség és a gazdag

²⁹ Szövetségi szinten az NII szabványosított szolgáltatásokat (pl. továbbítás, tárolás, biztonság, menedzsment) biztosító NATO és nemzeti kommunikációs infrastruktúrák és képességek összességét jelenti. A vízió megvilágítja, hogy a „föderáció” kifejezés tartalmilag eltér az eddig használatos „integráció”-tól, illetve a „hálózatok hálózata” kifejezést az NII váltja fel (NNEC VC 18. p.).

Ez az összetett megközelítés jól felismerhető Haig- Zsolt-Várhegyi István „információs infrastruktúra” magyarázatánál (p. 73-77.), illetve jó megvilágítást kap az infrastruktúrák globális - nemzeti - védelmi szintre történő tagozása és a kritikus infrastruktúra fontossága (p. 77-78.).

³⁰ NNEC VC 25-27. p..

tartalom mellett kihívásként jelentkezik az *interoperabilitás* és a *biztonság*.

Az Európai Községek Bizottsága a kutatás, a nyitott szabványok kidolgozásának elősegítésével, az érdekeltek párbeszédének támogatásával, illetve szükség szerint kötelező érvényű eszközök alkalmazásával kívánja ösztönözni az „egymással kommunikáló” technológiákat. Cél egy *biztonságos információs társadalmat célzó stratégia kialakítása*, ami egységes rendszerbe foglalja a rendelkezésre álló eszközöket, köztük az önvédelem szükségességével kapcsolatos *tudatosság erősítését*, a *fenyegetések folyamatos figyelését*, illetőleg a támadásokra és a rendszerhibákra való gyors és *hatékony válaszadást*. A bizottság állásfoglalása szerint támogatni kell a „beépített” biztonságra irányuló kutatásokat, és a személyazonosság-kezelés megoldását célzó alkalmazások bevezetését, és meg kell fontolni a szabályozás felülvizsgálatát, különösen a magánélet védelme, az elektronikus aláírás és az illegális és káros tartalom elleni fellépés területén.

Az információs és kommunikációs technológiákra vonatkozó kutatásokba történő befektetések és az innováció megerősítésének területei a *tudás*-, a *tartalom*- és a *kreativitás technológiái* (ideértve a kognitív, a szimulációs és a vizualizációs technológiákat is), a *fejlett és nyitott kommunikációs hálózatok*, a *biztonságos és megbízható szoftverek*, a *beágyazott rendszerek*, a *nanoelektronika*.³¹

Hasonló elemeket tartalmaz az e-kormányzat kialakítását célzó nemzeti stratégia. Az állampolgár-központú szemléletet célzó elektronikus kormányzat szerkezeti elemei a *közzszolgálati szektor intézményeinek belső működése* (back-office), a *lakosság és az üzleti szektor kommunikációja* ezekkel az intézményekkel (front-office), és a *köztük zajló kommunikációt biztosító hálózat*. A stratégia kulcsfontosságú feltételnek tekinti: az állampolgárok biztosak lehessenek abban, hogy működés és ügyintézés közben az adatok nem kerülhetnek illetéktelen kezekbe, illetve a személyek és dokumentumok megbízható hitelességgel azonosíthatók legyenek.

Ennek érdekében az e-kormányzati projektekre már a tervezési szakasztól kezdve be kell építeni a *személyes adatok védelmével kapcsolatos feladatokat*, ki kell alakítani a *megbízható hitelesítéshez* szükséges inf-

³¹ COM(2005) 229 végleges; i2010 európai információs társadalom a növekedésért és a foglalkoztatásért, 2-3. p.

rastruktúrákat és szabályozást, valamint ki kell alakítani egy *hálózat biztonságért felelős központi intézményt*, amely szolgáltatásaival (tanácsadás, riasztás, felvilágosítás) a közszférát és a magánszférát egyaránt támogatja.³²

A honvédelmi adatkezelő képességek nem vizsgálhatók a társadalmi információs környezettől elszigetelten³³ így újabb dimenzióként kell azonosítani a jogszabályokban meghatározott, közérdekből nyilvános adatokra vonatkozó *közzétételi kötelezettséget*, valamint a szervezeti érdekekből szükséges, *a nyilvánosságot célzó kommunikációs szükségletet*, illetve *a közigazgatási hatósági eljárások rendjébe történő részvétel*.

Az *elektronikus közzététel* az MH szervezeti struktúrája miatt összetett tevékenység, így szükség van az adatkezelő (az érintett szerv vagy szervezet), az adatközlő (a HM), és a honlap üzemeltető felelősségének általános meghatározására és a közzétételi folyamatra vonatkozó eljárásrend kialakítására.

A közzétételi folyamat kialakításának alapja az elektronikus információ szabadságról szóló 2005. évi törvényben meghatározott általános-, a jogszabályokban rögzített különös vagy egyedi közzétételi listák összeállítása.³⁴ Az életciklus elméletre támaszkodva meg kell határozni a közzétételre kötelezett adat megjelenésétől kezdve az engedélyezéshez szükséges eljárás lépéseit, meg kell határozni az engedélyezett adatok honlapon történő megjelenéséhez szükséges feladatokat, a helyesbítéssel, frissítéssel, eltávolítással illetve archiválással kapcsolatos feladatokat, az azokra vonatkozó biztonsági követelményeket és védelmi rendszabályokat, beleértve az illetéktelen beavatkozás esetén szükséges eljárásrendet, a jelentési kötelezettségeket, és a bizonyíték szolgáltatásra vonatkozó esetleges feladatokat. A Web oldalak könnyen támadás áldozatai lehetnek (pl. honlap tartalmának megváltoztatása, szolgáltatás megakadályozása, adatok törlése), így a szolgáltatások védelmére behatolás-érzékelő és riasztást végző megoldásokat kell alkalmazni, az adatbázis szerver védelméhez egyéb rendszabályokat kell rendelni (fizikai

³² E-kormányzat 2005 (E-kormányzat stratégia és feladatterv), 3. 4. p. és 4. 3. 2 p..

³³ Lásd Haig Zsolt – Várhegyi István már említett infrastruktúra felosztását (globális, nemzeti és védelmi információs infrastruktúrák).

³⁴ 2005. évi XC. törvény, 4. §. (2). A közzétételi listán szereplő adatok közzétételéért, folyamatos hozzáférhetőségéért, hitelességéért és az adatok frissítéséért az adatközlő felel (attól függetlenül, hogy saját honlapot üzemeltet, vagy közzététel céljából szolgáltatót vesz igénybe).

védelem, korlátozott számú hozzáférés engedélyezése, az oldalak automatikus frissítése, a problémákra gyorsan reagáló képességek kialakítása). Ezek a feladatok a Magyar Honvédség szervezetei mellett Internet szolgáltatóknál is jelentkeznek, amely esetekben a szolgáltatás rendelkezésre állásával, vagy a közzétett adatok sértetlenségével kapcsolatos követelményeket szolgáltatási szerződésben (service level of agreement; SLA) kell meghatározni.

A közérdekből nyilvános adatok hozzáférhetőségének biztosítása mellett egyre összetettebb feladat a minisztérium (és egyéb szervezetek/szervek) kommunikációs céljait szolgáló adatkezelő képességek/lehetőségek biztosítása. *Külső kommunikációként* szükség van a lakossági bizalom és megértés fenntartására, a *műveleti és krízis kommunikáció területén* a missziók kommunikációs támogatására, valamint *belső kommunikációs területen* a hiteles tájékoztatást, a bizalmi légkör kialakítását és fenntartását, valamint a közösségek hatékony működését kell támogatni.³⁵ Ez a tevékenység az adatok sértetlenségén kívül felveti *tartalom felügyelet* fontosságát.

Hazánkban a hatóságok (eltérő rendelkezés hiányában) a közigazgatási hatósági ügyeket elektronikus úton is intézik.³⁶

A hatóság a kérelem beérkezéséről értesítést küld, tájékoztat az esedékes illetékről. A hatósági ügyintézés során biztosítani kell az ügyfél betekintési jogát (és másolatkészítési lehetőséget), valamint a folyamatban választási lehetőséget az elektronikus és a hagyományos ügyintézés között. A hatósági döntés minősített aláírással hitelesített dokumentum. Az együttműködésre vonatkozó követelmény, hogy összetett, több hatóságot érintő ügyintézés esetén az érintett szervezetek a már rendelkezésre álló adataikat egymás felé biztosítják, és nem kötelezhetik arra az ügyfelet. Általános követelmény, hogy a hatóságnak gondoskodni kell az eljárás során megismert, törvény által védett titok (a továbbiakban: védett adat) és a hivatás gyakorlásához kötött titok (a továbbiakban: hivatásbeli titok) megőrzéséről és a személyes adatok védelméről. A

³⁵ 7001/2006. (HK 4.) HM irányelv a Magyar Honvédség kommunikációs feladatairól, II. fejezet, 1-3. p.

³⁶ A közigazgatás korszerűsítését szolgáló aktuális e-kormányzati feladatokról szóló kormányrendelet a Ket. körén belüli szolgáltatásokat négy szintre bontja (legalacsonyabb szint a csak elektronikus tájékoztatás, legmagasabb szintű (on-line) szolgáltatás a közigazgatási döntés elektronikus közlése és elektronikus illetékfizetés), és a különböző hatósági eljárások kialakításához prioritásokat állít fel (1044/2005. (V. 11.) Korm. rendelet 1. a. pont).

hatóságnak biztosítani kell az ügyintézési útmutató elérhetőségét, letölthető formában a szükséges formanyomtatványokat, valamint interaktív szolgáltatásként lehetővé kell tennie a határidőkkel, hatályos jogszabályokkal, az ügyfelek jogaival kapcsolatos információk elérését, tájékoztatást kell adni az adatvédelemről, illetve az egyedi azonosító használatáról, illetve az elektronikus ügyintézés technikai szabályairól.³⁷

2. A megvalósulás kezdeti lépései

Az elméleti kutatások, perspektivikus elképzelések, általános követelmények gyakorlatba ültetését jelenti, hogy a honvédelmi miniszter 2006. évi irányelvei között haderő fejlesztési prioritást kapott a *híradó és informatikai terület fejlesztése* (úgy, hogy az alapul szolgáljon a kialakítandó hálózat alapú hadviselési képességhez), a *telepíthető vezetési-irányítási rendszer fejlesztése* a műveleti részvételre tervezett szervezetek részére, illetve a haderő professzionális jellegének erősítése érdekében a *vezetési rendszer racionalizálása, fejlesztése*.

Általános haderő fejlesztési követelmény a szövetségi, EU, vagy egyéb koalíciós műveletekben való részvétel érdekében a kompatibilis vezetési, kiképzési és alkalmazási elvek kialakítása és a bárhol telepíthető tábori híradó-informatikai háttér megteremtése, valamint a minősített időszaki és a békevezetési rend eltéréseinek a legszükségesebb mértékre történő csökkentése. Az új típusú kihívásokkal való lépéstartáshoz elengedhetetlen az adatok gyűjtése, feldolgozása és a felhasználókhoz való időbeni eljuttatása, amelynek érdekében folyamatosan fejleszteni kell az információgyűjtés és feldolgozás hatékonyságát.

A prioritások között szerepel még a Magyar Honvédség *hálózat alapú hadviselési képességének* kialakítására vonatkozó terv kidolgozása, melynek során először a repülőgépek és a légi vezetési-irányítási rendszer közötti kapcsolat elemeit kell kialakítani, majd a képességet ki kell terjeszteni a szárazföldi csapatokra is.³⁸

Az ezredfordulót megelőzően különböző programok keretében megkezdődött a rendelkezésre álló távközlő és informatikai hálózatok fejlesztése, illetve a lehetséges integrációk előkészítése, és dinamikus terjedő, szervezeti határokat átlépő hálózatok jelentek meg. A különböző alrendszerek egy része napjainkra már egy *korszerű MH szintű transzport há-*

³⁷ Ket. 160. §, 30. §. 1-2, 17. §. és 160. §.

³⁸ A Miniszteri Irányelvek a védelmi tervezésről (2007-2016) szóló 10/2006. (HK 4.) HM utasítás 2. §.

lózatra csatlakozik, és körvonalazódik egy integrált, korszerű hálózat-felügyelet alapja. Az MH Iroda-automatizálási Program beindításával megkezdődött az egységes infrastruktúra által biztosított alkalmazások kialakítása (beleértve a portál rendszerű irodaautomatizálási rend kialakítását is). Ennek következtében látható, hogy a katonai szervezetek igényeit – a TCP/IP típusú hálózatot előrejelzők elgondolása szerinti – MH szinten menedzsel, egységes hang és adat kommunikációs hálózat fogja kiszolgálni.

A tervek szerint a tábori és az állandó infrastruktúra a felhasználók felé egységes kommunikációs felületet biztosítson, amibe bele kell érteni azt is, hogy a harci, békefenntartó vagy válságkezelő feladatok végrehajtásához az állandó és a tábori infrastruktúrának megfelelő csatlakozási képességet kell biztosítani a mobil felhasználók felé is.

A korszerű igények kielégítése érdekében körvonalazódni látszik a minősített adatok elektronikus kezelésére vonatkozó *egységes infrastruktúra* kialakítását célzó vezetői akarat. A felhalmozódott tapasztalatok lehetővé fogják tenni, hogy a NYÍLT, NEM NYILVÁNOS adat kezelő képességeket biztosító *zártcélú hálózat transzport-hálózatként biztonságosan kiszolgálja a MINŐSÍTETT adatok kezelésére feljogosított hálózatot is.*

Az egységes hálózat kialakítására irányuló törekvés mellett napjainkban és a közeljövőben még gyakorlati, vagy biztonsági okokból (pl. egy szűk felhasználói kör speciális adatfeldolgozási szükséglete, vagy minősítési/kezelési jelzés miatti elkülönítési kényszer) továbbra is meg kell, hogy maradjanak egyes helyi adatfeldolgozó képességek. E nyilvánvaló esetben is alapelveként kell kezelni, hogy *ezeket az elkülönített képességeket is egység szemlélet alapján – az MH hálózatosított szolgáltatásai-val összhangban – kell kialakítani és fenntartani* (amely követelmény a védelmi rendszabályokra is vonatkozik).

Az említett jelenségek mellett megjegyzendő, hogy a különböző információs rendszereket üzemeltetők és alkalmazók számára jelenleg *nem azonosan értelmezett az MH szintű szolgáltatásokra értendő egységesítés.* Egy homogén hálózat kialakítása anyagi okok miatt elképzelhetetlen, így a hangsúly a szervezetek által üzemeltetett, a szervezeti határokat gyakran átlépő *rendszerek összefogásán, a minimális szolgáltatások egységesítésén, a támogatási feladatok centralizálásán van.*

A heterogén hálózat működésének megértésében a NNEC szövetségi szinten alkalmazott „federation of systems” kifejezésre hivatkozom, ami jelzi, hogy az információs szükségletek kielégítése érdekében a különböző *szervezeti felelősségek nem szűnnek meg* (pl. a különböző alkalmazásokért, szolgáltatásokért való felelősségek nem ruházhatók át minden esetben egy központi szervezetre). A rendelkezésre álló technikai, humán, pénzügyi, információs erőforrások közös menedzselésével a szolgáltatási színvonal (és a biztonság) növelhető, párhuzamosságok szüntethetők meg.

3. Perspektivikus követelmények

A bemutatott szervezeti elvárások és általános követelmények alapján az MH szervezeti céljai támogatása érdekében az elektronikus információ biztonsággal szemben támasztott perspektivikus követelményeket a következőkben látom:

A biztonsági célok megvalósulása érdekében alapvető kérdés, hogy a technikai fejlődés által biztosított lehetőségek és az eddigi széttagolt rendszereket összefogó, egységesen kezelt hálózatra való törekvés igénye ne kerüljön szembe a kezelt adatok és az adatkezelő képességek biztonsági követelményeivel.

Az MH elektronikus adataival és adatkezelő rendszereivel kapcsolatos biztonsági célok, alapelvek és védelmi rendszabályok harmonizáljanak a szervezeti célokkal és külső, belső információs környezettel.

A biztonság érdekében kialakított hardver, szoftver elemek, adminisztratív eljárások olyan azonos technikai és szervezési alapelveken nyugodjanak, ami támogatja az egységes fenntarthatóságot, menedzselhetőséget és költséghatékonyságot.

A védelem továbbfejlesztésekor a kor követelményeinek megfelelően történjen meg a nyílt forráskódú megoldások alkalmazásának vizsgálata, lehetőségeinek felhasználása, szélesedjen a korszerű rejtjelző megoldások alkalmazása, valamint korszerű azonosítási és hitelesítési eljárások kerüljenek alkalmazásra.

A biztonsági alrendszerek fejlődése kövesse az igények fejlődését (adatfeldolgozási sebesség, mennyiség, közel real time követelmény), és erőforrás takarékos megoldásokat alkalmazzon.

A nemzetközi gyakorlatnak megfelelően hatékony visszatartó erőként kerüljön előtérbe az illegális tevékenységre utaló bizonyítékok gyűjtése és a szolgáltatása.

Az elektronikus adatkezelő képességek biztonságának MH szintű felügyelete, belső ellenőrzési rendje a tervezésért, üzemeltetésért felelős szervezeti elemektől függetlenül, korszerű eljárásokkal támogatva működjön.

A korszerű információ technológia támogassa a központosított biztonsági felügyeletet, a biztonsági helyzet nyomon követését és legyen képes a szükséges ellenintézkedések foganatosítására. A decentralizált elemeken keresztül valósuljon meg a védelmi rendszabályok betartása és betartatása, növelve a központosított felügyelet hatékonyságát.

A védelmi megoldások továbbfejlesztése során az MH elektronikus információ biztonsági felügyeleti funkciót ellátó szervezeti elem szakirányítása szerint valósuljon meg a szervezeti erőforrások minél hatékonyabb alkalmazása és a nemzeti, nemzetközi biztonsági szervezetek tapasztalatainak felhasználása.

Az informatikai tervezésért, üzemeltetésért, valamint a védelmi alkalmazásokért felelős állományt specializált, az elméleti és gyakorlati kérdéseket egyaránt átfogó képzési és továbbképzési rendszer támogassa.

Az EU ajánlásoknak és a nemzetközi gyakorlatnak megfelelően az elektronikus adatkezelő képességek és azok támogatása területén a védelmi rendszabályok integráltan jelenjenek meg az infrastruktúrában, alkalmazásokban és folyamatokban.

Az elektronikus információvédelmi követelmények kialakítása során a nemzeti, NATO, EU adatok védelmére egységesített, a nemzetközi normáknak megfelelő rendszer alakuljon ki.

Felhasznált irodalom

Arthur K. Cebrowski, John J. Garstka: Network-Centric Warfare: Its Origin and Future, 1998, (How Can the Military Not Change?)

Hóka Miklós: Szenzorok háborúja, a hálózatközpontú hadviselés; UHSZ 2002/2

Szép József: A NATO új kezdeményezése: a hálózat nyújtotta képesség; UHSZ 2004/12. p. 75.

NATO Strategic Vision 2005
NATO Network Enabled Capability Feasibility Study, 2005.
NNEC Vision and Concept, 2006
Network Enabled Capability, JSP 777, edition 1
Munk Sándor: Az információs fölényről; HT 2001/3, p. 50-51.
Munk Sándor: A Magyar Honvédség informatikai interoperabilitási politikája; 2006. HT 1-2.
Haig Zsolt-Várhegyi István: Hadviselés az információs hadszíntéren, p. 255-266, és 174-179; Zrínyi kiadó, 2005, ISBN 963 327391 9

Sándor Magyar – Dr. Miklós Sándor:

The advantages and possibilities of the IP based telecommunication in peace support missions

Hungary's international commitments in military operations have increased after joining NATO. Among others our troops are present in the Provincial Reconstruction Team (PRT) in Afghanistan, in the Multinational Land Forces (MLF) in Kosovo, in the Guard and Security Battalion (GSB) in Kosovo, in the Military Police Contingent (MPC) in Sarajevo. As the number of the troops on missions is about 1000 at present, there is a great demand for most advanced technical support including questions of military telecommunications. Based on the above mentioned troops the size of the units performing mission activities varies according to the task and the donation.

There are some places where the telephone communications demand can be met by only a few lines even without a switch board, while in other places a great number of extensions may be needed.

In our lecture we are trying to seek the possibilities of applying IP technologies taking into consideration their efficiency and cost effectiveness.

The most important attribute of missions is the fact that the soldiers carry out the tasks outside their own country, most of the time on destroyed areas without telecommunications infrastructure, that is why they can rely on the local public service providers only to a small extent in most cases the local telecommunications infrastructure is damaged or completely destroyed. The unusually extreme weather conditions, which can have a negative effect from the point of view of telecommunications, can cause a problem for the troops and also for the installed technical equipment and devices. These extremes are mainly the significant temperature differences between night and day, but most often the extreme heat during the day. The installation of telecommunications and informatics system as well as their efficient operation and maintenance gains outstanding importance in every peace support mission as the greater need for information and the applications of higher transfer capacity are gaining ground. To achieve this goal it is vitally important to ensure managing bandwidth and to decide on and select the most suitable transfer possibilities and the installations using them. The protection and the encryption of the channels also need special attention. The digital war theatre requires the support of the multimedia applications of a greater bandwidth (video conferences, file transfers) along with higher safety demands and budgetary considerations. Currently the Hungarian Armed Forces mainly uses ISDN (Integrated Service Digital Network) technology in speech based telecommunications.

The ISDN operates in time multiplex mode that is the elements working synchronously at both ends of the channel carry out connect the channels. In comparison with the networks of the previous generation one of the qualities

of ISDN is that it is capable of transmitting voice, data and image information to the users due to the fact that signs are transmitted in a solely digital way. Applying developed devices we can use several services at the same time. In the ISDN system the transfer capacity of a channel is 64 Kbps. Depending on the number of the channels in the type of the connection there is basic rate access and primary rate access. The basic connection contains two independent circuit-switched "B" (bearer) channels and one "D" (data) channel of a speed of 16 Kbps. The two "B" channels can be united so the transfer speed will be 128 Kbps. The data channel transports the information needed for control and synchronisation, it also contains the call number. Where there are only a few users or if the transfer demand is low this connection form can be basically sufficient although this is not typical of mission environments. Two ISDN switch boards can be connected into network connection using basic rate connection to reach all the network functions. The number area of the two switch boards can be reached from each other as on inside extension. However only maximum two channels can be used at the same time for voice and data transfer. Because the speed of the channels is constant 64 Kbps at this speed video-conference services are not sufficient, the other side can only be viewed in slow not clear images. The primer rate connection is suitable for users with higher demands. This contains 30 "B" and 1 "D" channels. The 30 channel can ensure greater possibilities but in the case of missions it is extremely expensive to provide channels with 2 Mbps bandwidth in international connection. Video conferences can be transmitted in a good quality using this connection. Because of budgetary considerations the network connection among the ISDN switch boards can be implemented using the "D" and the necessary number "B" channels (below 30), on the other hand the cost effectiveness of "B" channels of constant speed of 64 Kbps can be regarded negative compared to IP (Internet Protocol) technology.

Besides the voice connection, it is very important to establish the computer connection with the missions. This connection must meet the high safety maintenance standards. When using WAN (Wide Area Network) the voice connection depending on special local conditions must be established according to the user's needs. The suitable solution for this is the VoIP (Voice over Internet Protocol). VoIP can substitute the traditional (ISDN) telephone lines. In contrast with traditional switch boards IP telephones are not necessarily connected to switch boards but to the computer network.

The transfer of voice through computer network can be done only by software installed to computer workstations or by IP switch boards as well. The IP system is capable to transfer video and fax signs as well.

The most well known IP application the Internet, which in the USA developed from ARPANET into worldwide network through a few decades. At the same time, companies are employing Intranet networks more and more often.

These systems also use Internet technology private networks. The Intranet mainly means a protected private network, which is isolated from the outside world.

The IP is situated in the 3rd (network) layer from the OSI (Open System Interconnection). In contrast with ISDN, it doesn't work in a circuit-switched way, which seizes the direct route between the source and destination for the time of the entire call and it directs every packet separately in a packet switched mode, that's the reason why it can be considered to be flexible. This also has some advantages and disadvantages.

As far as the IP disadvantages are concerned the delay in the applications of voice transfer due to the fact that the order of arrival of the IP packets is not guaranteed and packet losses can also occur. The delay depends on the distance between the two endpoints on the transfer possibilities on the route and the overload of the network.

One of the IP advantages is that they represent at the same time the services of the data and telephone networks. As the data, including voice, are transmitted in the form of packets, in the case of voice the 64 Kbps channel is not built in a direct way like with ISDN technology. Comparing the two previous solutions even 4-6 voice channels can be transferred on the same bandwidth depending on the compression or there is optimal bandwidth left for the data transfer besides the transfer of the two voice channels. In mission areas this is an especially good solution because the eligibilities (outgoing dials from the camp and operation area) are approved of based on strict security regulations and on the staff position. Because of all this only few voice channels can occupy the bandwidth at the same time this way providing higher capacity for the data transfer. Voice transfer on a lower bandwidth in international relation results in significant cost effectiveness.

Another advantage of the IP is that physically one unified network has to be built and maintained in the mission area.

The isolation of peace support areas in most cases enhances the satellite connection. In these areas basically satellite leased lines are established with restricted bandwidth. The use of dialled satellite telephone equipment (Iridium, Immarsat) – where the speed of the data transfer is low – is highly expensive, this can be operated only for secondary systems if the main connection form is not available. The optimal efficacy of the bandwidth is therefore more favourable for the IP systems.

Expenses can also be reduced – provided the task and the organisation allow – by not using a switch board. With IP telephoning one endpoint can directly connect to the other one so it is often sufficient to use gateways and routers instead of a switch board. Outgoing calls from the network can be made through VoIP gateways in this case. Taking into consideration all the

above mentioned, in many instances the efficiency of the military telecommunications system is increased by the IP switch board.

Data transfer on such large scale – including VTC (Video Tele Conferencing) and e-mails – outweighs traditional voice and fax services more and more. VTC can be established also based on ISDN technology, when in a circuit-switched way one installation dials the other one (most of the time through basic rate access ISDN), but also with the help of routers using the informatics system.

The scale of the telecommunications equipment used for IP telephoning is extremely large. The services of IP telephoning connected to the computer network or to the IP switch board physically resemble the ISDN equipment. There can be differences also in the interface type as the IP telephone can be connected to the computer through Ethernet and USB. However, many times not even a telephone set is needed because the computer workstations are capable of performing the telephone service based on software using a sound card. By extending the microphone and speaker through radio interface there is a possibility for making phone calls but using this way mainly especially in such areas is obviously not allowed by the security measures.

As in every telecommunications and informatics system and network, network management is outstandingly important. The tasks of network management are numerous:

- fault management;
- configuration management;
- administration management;
- performance management;
- security management.

The monitoring network can find the weak points and can shorten the reaction time.

From the point of view of network management the centralised management of the IP systems can be solved. The elements of the informatics network (servers, routers, switches, fire walls, VPNs) continuously generate the log files and fault messages the analyses of which can increase the safety of the network.

The management of the telecommunications equipment is carried out in the network management:

- establishing a constant connection (on-line), in this case the quantity of the management data must be optimized and it cannot exceed the “regular” data transfer;
- using temporary connection (off line) for example dialling another route using PSTN (Public Switched Telephone Network).

Continuous connection ensures higher performance that's why it is used as a primary management solution but if the constant management is disrupted the management function must be carried out on secondary routes.

Due to the fact that the experts of the centralised network management possess the greatest amount of knowledge about the network level management, it is necessary to integrate the IP network situated in the mission area into the management system of the closed purpose network of the Hungarian Defence Forces. At the same time, the system manager of operational area has to be ready to solve the local problems because, as a result of the extreme conditions, there is a greater chance for problems and faults. Concerning hardware, the manager is supposed to have extra amount of repair material in stock since the transport and supply of the repair materials can take a long time, depending on the actual scene, it can last for several weeks or months.

In conclusion, the everyday work of the soldiers serving in peace support operations is hindered and sometimes even made impossible by the lack of the properly operating telecommunications and informatics system and of the connection to their own nation. This fact makes safe operation and maintenance vitally important. The effective employment of the bandwidth available supports the use of the IP technology in contrast with the ISDN technology.

References

- Magyarné Kucsera Erika: A hálózatzfelügyelet és lehetőségei a Magyar Honvédség híradó szolgálatánál, ZMNE Tudományos Diákköri Konferencia 2000.
- Tannenbaum-Andrew S.: Számítógép hálózatok, BP.- Novotrade kiadó Kft.-1992.
- Dr. Molnár S: IP hálózatok forgalmi méretezése, MAGYAR TÁVKÖZLÉS 2000/9 (XI. évfolyam 9. szám)
- Grünzweig T.-Sziklai A: Intelligens szolgáltatások IP hálózaton, MAGYAR TÁVKÖZLÉS 2000/5 (XI. évfolyam 5. szám)
- Balogh Tamás: Az ISDN felépítése, ISDN szolgálatok, szolgáltatások és alkalmazásai, BP. – PKI-FI Adat és Kommunikációs Osztály 1994.
- www.honvedelem.hu

Balázs Pándi

Reformation of the military core networks

1. Features

The policy of the organization is primarily concerned with defense, thus the importance of communications systems have increased in the armies of NATO member countries. One of the reasons for this is that in such a situation the pre-installment of communications on field of operations plays an important role. The second reason is that the communications requirements of the military and political leadership have increased in both quality and quantity. The third reason is that the field communications system has to be connected to the stationary military communications system at as many points, and as high bandwidth as possible [1]. The network of the Hungarian Defence Forces currently consists of the following two (considerably independent) subsystems:

- the stationary communications systems of the Hungarian Defence Forces³⁹
- the national computer backbone network⁴⁰

In the computer system of the Hungarian Army the development of the computer infrastructure and systems minimally required for our NATO membership on a top- and mid- management level has taken place between 1999 and 2003, and from 2004 the extension of the stationary network towards the member countries has started. The military leadership considers high priority future task, the creation of an extensive, unified computer system of the Hungarian Army, the technical basis of which would be the long-range data transmission backbone network (transport network) of the Hungarian Defence Forces [2].

The integration of the telecommunications and computer networks on a technological level is one of the prime concepts concerning the communications systems of the defense sector.

³⁹ the stationary communications system consists of communications centers placed at different military installations and the communications lines which connect them. The communications centers are directly connected with the public telecommunications networks. The lines of communication are installed on the basis of the stationary military networks. The first series of digital switch centers providing ISDN services has been installed in 1999, when our country became a member of NATO. The wired transmission routes of the system today are also mainly provided by lines leased from public service providers. Besides this an equivalent nation-wide microwave network is simultaneously operated.

⁴⁰ the organization of the defense sector typically operates computer networks, which require minor transmission routes, operate independently, and employ local and long-distance network resources.

After examining the environment of the Hungarian Defence Forces it can be stated that (according to our countries' commitment to NATO) its' external connection point is the NATO ICIS⁴¹.

The continuously increasing demands of military users for transferring, displaying, and processing information drive communications developments towards broadband applications.

The communications system of NATO consists of for parts:

- integrated military communications system owned by NATO
- military communications system owned by the member states
- public (national and international) communications systems supporting the connection between the NATO system and the system of the member states
- digital transmission infrastructure connecting the variously owned communications systems

Considering the networks above, most of the member states have already begun to modernize and adapt their national communications network⁴², in order to reach a bandwidth between 155 Mbit/s and 2.5 Gbit/s. From this point of view the integration demands of the communications system of the Hungarian Army are reasonable and timely.

2. Managing the network of the Hungarian Defence Forces

Guidance about who should be involved in the management and operation of the current network, is given by the appropriate legislative provision, the Organizational and Operational Regulation of the Ministry of Defense, and staff measures⁴³. After the reorganization of the Ministry of Defense, the administrator of the private telecommunications network is the Communications and Computer Command of the Hungarian Defence Forces, which is commanded directly by the General Staff of the Hungarian Military. Concerning the administrative activities Gáspár Szűcs PhD has mentioned in a previous lecture that: *"The individual group commands, units, background institutions, develop their computer applications independently, which makes the cooperation of these systems and their integration into the Army computer network significantly more difficult"* [3]. According to the appropriate special instruction the network of the Hungarian Army has a three level operational and technical administration structure. The National Network Administration Center created within the organization of Communications and Computer Command of the Hungarian Army integrates the group of activities on the highest level. The Regional Network Administration Centers function on the middle level. The

⁴¹ the C3 system supporting the command of NATO

⁴² optical fibre, ATM, SDH and IP based

communications centers and administration centers of the individual military units are on the bottom level. The system is completed by the Reserve National Network Administration Center, which functions under the command of the Communications and Computer Command of the Hungarian Defence Forces. The operation of the network relies highly on public service providers, other communications providers, besides which communications maintenance teams were set up for handling smaller volumes of maintenance and troubleshooting tasks. Centralization and normative regulation are the main characteristics of the network of the Hungarian Army. Only a few organizations within the military take part in the financing of the network of the Hungarian Army.

3. Development directions

In military scientific circles there is still debate on the basic technical platforms, and organizational questions of the integration and development. Sándor Szöllösi has formed the following expert opinion: *"In the homeland we should aim to: a.) set up a common communications and computer infrastructure requiring small investment and operational costs, b) not necessarily set up an autonomous national communications infrastructure, but to rely on the networks of certified (especially from a security point of view) civilian providers, because their technical possibilities exceed our current and probably also our long term requirements..."* [4]. Concerning the modernization of the military communications system Károly Fekete PhD made the following observations: *"Considering the developments in the communications system of NATO, the most recommended solution for the technical upgrading of the Stationary Telecommunications System of the Hungarian Army would be the introduction of MPLS/ATM VPN technology. The most efficient method for this would be the establishment of public DWDM-SDH-MPLS/ATM-TCP/IP infrastructure and virtual private networks.[...]"*

The final recommendation would be that, the most efficient way to upgrade the Stationary Telecommunications System of the Hungarian Defence Forces would be to establish a high speed communications system, based on the advanced public communications infrastructure, which first extends, than replaces, the current stationary communications system, is backward compatible with it, is capable of transferring all media types, is fully integrated on a technological and organizational level in terms of the telecommunications and computer networks, and is capable of setting up a virtual private network." [5].

Both publications show a vision of an integrated, but not necessarily autonomous communications system. The main reason for giving up the autonomy, is that the operators of the public networks (because of their market interests) are able to and are forced to, keep up to the accelerated rate of international development of telecommunications and information technology, which was not

true for the various organizations of the state administration (especially the Hungarian Army) in the past 15 years. When determining the directions for the future developments of the Network of the Hungarian Defence Forces, the NCW (network centered warfare) conception developed by the United States Department of Defense also has to be taken into account, which has been adapted and applied under the name NNEC (NATO Network Enabled Capability). The point of the concept is that all the organizations and personnel taking part in the military operations should be able to access all the information needed to complete their tasks, in the appropriate place, time content structure, and format. This is provided by such a communications network that is capable of transferring, processing, and providing the information requirements, which can occur at different points of the network, simultaneously, or almost simultaneously, in highly varying quantities. Sárdor Hamar made the following observations about the concept of NNEC: *“Reaching the NATO Network Provided Capabilities is a long process, the results of which could first arise in the next decade. [...] The concept contains many such requirements, that none of the currently applied military communications and computer systems can completely fulfill: [...] It is an important question whether the communications and computer infrastructure, which is currently under development provides a proper basis for establishing such a system, or whether it is necessary to alter the long term concepts.”* [6]. The current military communications system has to be upgraded, adapted according to the NATO requirements. Today only the strategic direction of development is known, thus the question of what are the appropriate technological platforms, and the majority of organizational questions are still open.

4. Summary

After examining the above, I have come to the conclusion that the Network of the Hungarian Defence Forces has to fulfill such special military communications requirements, which make it special even within the family of private networks. Due to the dislocation of military organizations, its topology significantly differs from the topology of systems providing service for the organizations of the state administration. Due to our country's NATO membership the requirements specified by NATO affect the development and adaptation of processes more significantly. These requirements do not primarily arise from the demands of the civilian and law enforcement administration. The technological-organizational solutions currently applied at the Network of the Hungarian Defence Forces enable it to interact with various communications systems, thus on this level it can serve as the basis of a possible integration process with the Electronic Governmental Backbone-network, however because of its significant difference (due to its function) its role should be assigned according to the defense administration tasks of the Government.

References

- [1] Fekete, Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, PhD dissertation, Zrínyi Miklós National Defence University, Budapest, page 40, 2003
- [2] Szűcs, Gáspár (PhD): A Magyar Honvédség informatikai helyzete, fejlesztési tervei, problémái, „Communication 2003” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86229 6 2, page 370-373, 15th October 2003
- [3] Szűcs, Gáspár (PhD): A Magyar Honvédség informatikai helyzete, fejlesztési tervei, problémái, „Communication 2003” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86229 6 2, page 376, 15th October 2003
- [4] Szöllősi, Sándor: Az új típusú haderő és a súlypont-átrendeződés kérdései a technikai struktúrában, „Communication 2003” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86229 6 2, page 375, 15th October 2003
- [5] Fekete, Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, PhD dissertation, Zrínyi Miklós National Defence University, Budapest, page 120-121, 2003
- [6] Hamar, Sándor: Új kihívások a katonai információs rendszerekkel szemben, „Communication 2004” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86441 5X, page 124-126, 15 th September 2004

Bibliography

- [1] Fekete, Károly: Towards a new generation of WLAN in military communications, „Communication 2005” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 7060 11 1, page 334-340, 27th October 2005
- [2] Magyarné Kucsera, Erika: A teljes integráció fontossága az MH zártcélú infokommunikációs hálózatainak menedzsmentjében, „Communication 2005” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 7060 11 1, page 199-202, 27th October 2005
- [3] Sándor, Miklós (PhD) – Farkas Tibor: A honvédség állandó hírhálózata fejlesztésének kérdései, Kard és Toll, Vol 2006/2, Budapest, ISSN 1587-558X, page 158-164, 2006

Maros Dóra

Veszélyhelyzeti távközlés

Bevezetés

A statisztikák azt mutatják, hogy a XXI. század első évei alatt jelentősen növekedett a különböző típusú veszély- és katasztrófa-helyzetek (természeti katasztrófák, terroristatámadások, balesetek stb.) bekövetkezésének valószínűsége, és e tendencia nem változik kedvező irányban. A bekövetezett katasztrófa-helyzetben a távközlési hálózatok sérülése, vagy túlterheltsége miatt – ha időszakosan is – de megszakad az emberek közötti kapcsolat, a telefonálás, a segélykérés és a mentési munkákat szolgáló információk közlése sokszor lehetetlenné válik. A távközlési rendszerek működésképtelensége megbénítja az országon, vagy régióon belüli, néhány esetben a katasztrófa-ban érintett országok közötti kommunikációt, ezért a megteendő intézkedések nemzeti és nemzetközi szabályozása a legtöbb esetben létfontosságú feladat. Ugyanakkor a távközlési erőforrások üzemképes működése elengedhetetlen a veszély- és katasztrófa-helyzet előrejelzése, a segélykérés, vagy a mentési feladatok megszervezése során, különös tekintettel a különböző típusú készenléti szervezetek együttműködésére, mint például rendőrség, polgári védelem, mentők, tűzoltóság, katasztrófavédelem stb.

Az utóbbi pár évben (de legfőképpen a 2001. szeptember 11-i terrortámadás óta) a világban olyan új fogalomkör terjedt el a távközlést érintő műszaki és szabályozási kérdésekkel foglalkozó szakemberek és testületek körében, amely egységbe foglalja a válsághelyzetekhez kapcsolható távközlési területeket. Angol megnevezése: *emergency telecommunication*, magyarul *veszélyhelyzeti távközlés*. A *veszélyhelyzeti távközlés* fogalmát a következőképpen lehet meghatározni: minden olyan tényező (amely lehet műszaki, jogi, emberi, szervezési, mentési, helyreállítási stb.), amely veszélyhelyzet esetén összefüggésbe hozható a távközlési, hírközlési, informatikai szolgáltatásokkal és hálózatokkal.

Az EU, a NATO és a nemzetközi civil és szakmai testületek összefogásával jelenleg olyan nemzetközi szabályozási környezet kidolgozása folyik, amely definiálja a veszélyhelyzeti távközlés egyes területeit érintő műszaki és szervezési teendőket, különös tekintettel a polgári lakosság és a készenléti szervezetek válsághelyzeti kommunikációjára. Magyarországon a veszélyhelyzeti távközléshez kapcsolódó nemzetközi előírások, feladatok teljesítéséhez szükséges a hazai távközlési szolgáltatók bevonása, eszközeik és szolgáltatásaik igénybevétele. Ugyancsak fontos kérdés, hogy a magyar szabályozási környezetben olyan jogszabályok jelenjenek meg, amelyek előírják a hazai távközlési infrastruktúra megbízható működésének feltételeit, válsághelyzetekben azok helyreállításának, együttműködésének megszervezését, valamint a döntési és felelősségi köröket. Szükséges azonban az állami tartalékgazdálkodás racioná-

lisabbá tétele és összehangolása abban az értelemben, hogy a tartalék eszközök a távközlési szolgáltatóknál folyamatosan készen álljanak.

Veszélyhelyzet esetén sokszor csak egyedi döntés alapján lehet és kell a szükséges és lehetséges feladatokat meghatározni. Az állami szervezetek közötti kapcsolat alapja a kölcsönös egyeztetés, megegyezés és tervezés.

A veszélyhelyzeti távközlés szabályozási területei

A Tamperei Egyezmény

A veszélyhelyzeti időszakra vonatkozó nemzetközi távközlési együttműködés elveinek kidolgozása az ENSZ keretében működő Nemzetközi Távközlési Unió (ITU) 1991-ben rendezett konferenciáján kezdődött. A nemzetközi távközlési együttműködés elvei a több lépcsőben egyeztetett, illetve kidolgozott, *“Tamperei Egyezmény a Távközlési Erőforrások Biztosításáról Katasztrófa Elhárítás és Mentés Céljaira”* nemzetközi egyezmény tervezetében öltöttek formát. Az Egyezményt harminc ország aláírásával 2005. január 8-án ratifikálta az ENSZ, amelyhez hazánk is csatlakozott. A Tamperei Egyezmény segítségnyújtási alapelve, hogy a katasztrófa következményeinek felszámolásához az államok a távközléshez szükséges személyzetet, felszerelést, anyagot, információt, oktatást, átviteli hálózatot, illetve kapacitást, továbbá a távközléshez szükséges minden egyéb forrást biztosítanak egymásnak. A nemzetközi segítségnyújtásban résztvevő államok mentőcsapatai számára az Egyezményben foglaltak alapján biztosítani kell:

- az intézkedések hatékony megtételéhez a szükséges távközlési berendezések akadálytalan és azonnali telepítését;
- pontos és aktuális információk közlését az eseményről, a katasztrófa helyéről és az érintett körzetekről;
- minden rendelkezésre álló erőforrás telepítésének és használatának koordinálását;
- a katasztrófakörzeten kívül eső helyekről mindenfajta információ azonnali elérését, valamint az érintett terület(ek)en tartózkodó emberek biztonságát és védelmét.

A katasztrófában érintett és a nemzetközi segítségnyújtást igénybevevő államoknak az Egyezmény értelmében biztosítaniuk kell:

- a mentésben résztvevő csapatok, egységek azonnali telepítését (elhelyezését, ellátását);
- a mentéshez szükséges logisztikai háttérrel és infrastruktúrával;
- a helyi és nemzetközi mentőalakulatok közötti szoros együttműködést;
- a nemzeti és nemzetközi mentésben résztvevők közötti kommunikációra használt távközlési rendszerek és berendezések kompatibilitását.

EU-s szabályozások

Magyarország az EU-hoz történő csatlakozásával kötelezte magát az EU szabályozási rendszerével harmonizáló jogalkotás végrehajtására. Az EU-s szabályozások közül a veszélyhelyzeti kommunikáció tekintetében három irányelvben és egy ajánlásban találunk a területre vonatkozó előírásokat. A három irányelv a következő: Keretirányelv (Framework Directive 2002/21/EC), Egyetemes szolgáltatási irányelv (Universal Service Directive 2002/22/EC) és az Elektronikus kommunikációs adatvédelmi irányelv (Privacy Directive 2002/58/EC). A fenti három irányelvben megfogalmazott előírások megalkotásához az EK Bizottsága az Európa Tanácshoz és az Európai Parlamenthez írott közleménye adja az alap-dokumentumot, amelynek címe: *Civilek védelme – A lehetséges veszélyhelyzetekre való felkészülési programok bevezetésének folyamata*. Az Európai Bizottság 2003/558/EC (Commission Recommendation) ajánlása ugyanakkor részletesen szabályozza a helyadatokkal kiegészített segélyhívások (E112) feldolgozásának és továbbításának elveit és szabályait az elektronikus hírközlési hálózatokban.

ITU és ETSI szabályozások

A Nemzetközi Távközlési Unió (ITU) számos munkacsoportja foglalkozik a veszélyhelyzeti kommunikáció szabályozási kérdéseivel, és a szükséges szabályozási rendszer létrehozásával. Az ITU két alapvető irányban határozta meg a részletesen kidolgozandó területek körét:

- 1) Közcélú (nyilvános) mobil hálózatok használata a lakossági riasztás és segélykérés céljaira.
- 2) Hálózatok együttműködése krízishelyzetekben, prioritásos hívások működésének biztosítása.

Az ITU több olyan ajánlást (recommendation) dolgozott ki, amelyek szorosan kapcsolódnak a fenti területekhez. Az egyik ezek közül az *ITU-R M.816 Ajánlás* amely a segélyhívások alkalmával a felhasználó helyének pontos meghatározásával összefüggő információk (location information) felhasználását írja le mobil rendszereknél. A dokumentum ugyanakkor a személyes adatok védelmére is hangsúlyt fektet, ezért az ilyen jellegű információk kezelését, esetleg kiadását csak az arra jogosult szervezetek számára teszi lehetővé.

Az Európai Távközlési Szabványügyi Intézet (ETSI) keretein belül, az európai szabályozások megalkotásában három szakértői csoport vesz részt: az EMTel, a TIPHON és a 3GPP. A TIPHON a Közcélú Kapcsolt Távközlő Hálózat (PSTN) és az IP alapú csomagkapcsolt infrastruktúra konvergenciájához szükséges együttműködési paramétereket írja le. A 3GPP a harmadik generációs mobil rendszerek fenti vonatkozású szabványainak kidolgozását végzi. Az EMTel csoport feladata, hogy javasolja, támogassa, és tevékenyen segítse a veszélyhelyzeti távközlésre vonatkozó szabályozások (szabványok, direktívák, együttműködési megállapodások, ajánlások) kidolgozását, valamint

figyelemmel kísérje a témához kapcsolódó, de nem ETSI hatáskörön belül történt eseményeket, és kiadott dokumentumokat.

Az EMTEL jelenleg hat olyan nagyobb terület szabályozási kérdéseivel foglalkozik, amelyek a veszélyhelyzeti távközléshez tartoznak. Ezek a következők:

- TS 102 180: A lakosok hatóságokkal / szervezetekkel történő kommunikációjának követelményei szükséghelyzet esetén (segélyhívások kezelése)
- TS 102 181: Szervezetek közötti kommunikáció követelményei veszélyhelyzetekben.
- TS 102 182: A szervezetektől a lakosság felé irányuló kommunikáció követelményei veszélyhelyzetben (riasztás).
- TS 102 410: A lakosok közötti kommunikáció követelményei veszélyhelyzet idején
- TR 102 444: AZ SMS és CBS (Cell Broadcast Service) alkalmazása riasztási üzenetek küldésére veszélyhelyzetben
- TR 102 445: A veszélyhelyzeti kommunikációs hálózatok rugalmassági követelményei.

A nemzetközi szabályozások tanulmányozása alapján három olyan nagyobb szabályozási területcsoportot lehet azonosítani, amelyek közvetlenül meghatározzák a veszélyhelyzeti távközlés működését (ld. 1. ábra). Ezek a következők:

- civileket érintő kommunikáció (I. csoport)
- szervezeteken belüli és szervezetek közötti kommunikáció (II. csoport)
- távközlési hálózatok működését biztosító tényezők (III. csoport)

Az első csoportba sorolt, civileket érintő területek a riasztás, a segélykérés, és a civilek közötti kommunikáció. A telefonon keresztüli riasztás már számos európai országban működik és a helyadatokkal kiegészített 112 (E112) hívások eddig több ezer ember életét mentették meg azokban az országokban, ahol ezt a rendszert már bevezették. Sajnos Magyarországon jelenleg sem a telefonos riasztás, sem az E112 nem működik.



1. ábra. A veszélyhelyzeti távközlés szabályozási területei

A szabályozási területek második nagy csoportját azokhoz a telekommunikációs csatornákhöz lehet rendelni, amelyek az előkészítésben, mentésben és helyreállításban szerepet játszó szervezeteken belül, illetve az egyes szervezetek között jön létre. Ebbe a csoportba két nagyobb szervezeti típus tartozik: a készenléti szervezetek (mentők, tűzoltók, rendőrség stb.) és a kormányzati szervezetek (hatóságok, minisztériumok, polgármesteri hivatalok). Válsághelyzet esetén elsődleges fontosságú a kormányzati szervek és készenléti szervezetek közötti kölcsönös információátadás és együttműködés, ugyanakkor a veszélyhelyzeti távközlés egyes területeinek a koordinációját a szervezeteken belül és azok között is multilaterális szinten kell (kellene) biztosítani.

A harmadik és egyben legnagyobb terület a veszélyhelyzeti távközlés azon elemeinek a szabályozási köre, amelyek a távközlési hálózatok működésének feltételeit írják le válsághelyzetekben. Ebben a csoportba azok a műszaki szabályozási területek tartoznak, amelyeket elsősorban az EU, ITU és ETSI dokumentumok írnak le. A csoportba négy alapvető terület tartozik: hálózatok felügyelete, hálózatok együttműködése, forgalom átírányítás és kapacitásbővítés, valamint a tartalékolás és helyreállítás.

A veszélyhelyzeti távközlés magyarországi helyzete

Szabályozások

A magyarországi szabályozási környezetben a veszélyhelyzeti távközlést valamelyest érintő irányadó keretszabályozásoknak a következő törvényeket lehet tekinteni:

- 2003. évi C. törvény *az elektronikus hírközlésről (EHT)*;
- 2004. évi CV. törvény *a honvédelemről és a Magyar Honvédségről*;

- 1999. évi LXXIV. törvény (többször módosított) *a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről*

Az EHT-hez kapcsolódóan jelent meg a 100/2004. kormányrendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról. A kormányrendelet ugyan több kapcsolódó jogszabály megalkotását írja elő, azonban csak két olyan IHM rendelet született, amely konkrét területeket szabályoz. Ezek:

- 24/2004. IHM rendelet a védelmi feladatokban résztvevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról,
- 27/2004 IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről.

A 27/2004. IHM rendelet egyik pontja szerint a szolgáltatóknak a minősített időszakra történő felkészülés keretében saját szakmai feladat- és hatáskörébe tartozóan kell biztosítani a védelmi felkészüléssel, műszaki, forgalmi, katasztrófa vagy egyéb veszély miatt keletkező üzemzavar elhárításával kapcsolatos intézkedések kidolgozását, tervek készítését és azok folyamatos aktualizálását. A 24/2004 IHM rendelet pedig rögzíti, hogy a védelmi felkészülési feladatok végrehajtásáért minden esetben a szolgáltató vezetője felelős. A jogszabályok tanulmányozása után egyértelműen kijelenthető, hogy az érvényes jogszabályok nem biztosítják kellően sem a felkészülés, sem a minősített időszaki feladatok elvégzéséhez szükséges operatív intézkedési mechanizmust, csak feladatokat fogalmaznak meg, azok végrehajtásának módját nem. Nem egyértelmű és sokszor nem azonosítható a hatóságok jogalkotásban és döntésben vállalt szerepe és felelőssége sem.

Készenléti szervezetek kommunikációja

Magyarországon a készenléti szervek által még ma is használt URH diszpécser rendszerek már nem elégítik ki a készenléti feladatok ellátásához szükséges egyre növekvő kommunikációs feladatokat, és nem felelnek meg korunk kommunikációs rendszereivel szemben támasztott követelményeinek sem. A magyar Kormány az 1031/2003. kormányhatározattal rendelte el a készenléti és a kormányzati felhasználói kör rádiókommunikációs igényeinek kielégítése céljából, a Schengeni Egyezmény követelményeinek megfelelő, és az Európai Távközlési Szabványosítási Intézet szabványa szerint működő egységes digitális rádiótávközlő (EDR) rendszer kiépítését. 2005 októberében a Miniszterelnöki Hivatal EDR Kormánybiztosa és a T-Mobile Magyarország Rt. - Magyar Telekom Rt. konzorcium megkötötte az EDR létrehozására kiírt nyílt, kétfor-

dulós, tárgyalásos közbeszerzési eljárás szerződését. A TETRA szabvány szerint kiépült EDR jelentősen javítja az érintett szervek belső híradását, lehetővé teszi a szervek egymás közötti hatékony kommunikációját, ezzel nagymértékben hozzájárulva a reagáló képesség fokozásához, az együttműködés hatékonyságának növeléséhez. A teljes kiépítéssel Európa egyik legkorszerűbb és létszámarányában legkiterjedtebb készenléti rádiórendszere lesz 2007 elejére a hazai EDR.

Mivel karbantartás, meghibásodás, túlterhelés (esetleg más ok, pl. természeti csapás, robbantás) miatt a TETRA hálózat is néha kieshet, a készenléti szervezetek embereinek ilyenkor nem marad más kommunikációs lehetősége, mint a nyilvános mobil hálózatokat használni. A nyilvános mobil hálózatokban alkalmazható prioritásos híváskezelés erre is megoldást adhat, amelynek Magyarországon ma nincs még szabályozási háttere. A hívásprioritás kezelése különösen fontos lehet válsághelyzetekben, amikor a rendelkezésre álló távközlési erőforrások legszélesebb kihasználására van szükség.

A lakosság riasztása

A lakosság riasztása és megfelelő tájékoztatása veszély- és katasztrófhelyzetekben elsődleges fontosságú feladat az élet- és vagyonbiztonság megóvása érdekében. Az 1996. évi XXXVII. törvény a polgári védelemről 4.§ c.) pontja kimondja, hogy a lakosság figyelmeztetése, tájékoztatása és riasztása polgári védelmi feladat. A 38.§ (1) e) pontja pedig rögzíti, hogy a lakosság riasztását szolgáló berendezések telepítésének, fejlesztésének, karbantartásának és működésének fedezetét az Országgyűlés évente, a költségvetésről szóló törvény „Belügyminisztérium” fejezetében biztosítja.

Hazánkban a lakosság riasztása jelenleg három módon valósítható meg (60/1997. kormányrendeletet)

- szirénák megszólaltatásával (elektromos vagy kézi),
- médián keresztül (televízió, rádió),
- gépjárműre szerelt vagy fixen telepített hangosbeszélő bemonddással.

Magyarországon körülbelül 5000 db. elektromos sziréna áll rendelkezésre a lakosság riasztására, melynek többsége elavult (kb. 30 éves) és kézi indítású. A szirénák mai beállításai 4 hangjelet képesek kibocsátani, amelyek a következőket jelentik: „katasztrófariadó”, „légi riadó”, „veszély elmúlt” és „morgató jel” (sziréna próba). A lakosság döntő többsége nem ismeri a szirénajeleket, ezért azt sem tudja, hogy a sziréna megszólalásakor mi a teendője. Az erősáram kimaradása esetén a mai elektromos szirénák némák maradnak, míg a kézi szirénák hallhatósága csak töredéke az elektromos szirénáknak. A szirénahangok terjedése a II. Világháború óta lényegében nem került tömegesen kipróbálásra Magyarországon, pedig azóta az átlagos zajszint jelentősen emelkedett, és ezért a szirénák elméleti hallhatósági körzetei jelenleg a lakott területek töredékét képesek csak lefedni. A médiákon (televízió és rádió csa-

tornák) keresztül történő, veszélyre figyelmeztető hírek, jelzések csak bekapcsolt vevőkészülékek esetén juthatnak el az érintettekhez, (ami pl. éjszaka nem tipikus). A vevőkészülékek többségének működtetéséhez tápellátás szükséges, ezért áramkimaradás esetén töredékére csökken a működőképes berendezések száma. A rádió, televízió keresztüli riasztás ugyanakkor csak egyes műsorcsatornákra korlátozódik, melyeket adott esetben lakosságnak csak egy része (esetleg töredéke) figyel. A riasztás és tájékoztatás céljaira igénybe vehető hangosbeszélők átviteli sáv szélessége az érthetőségi határt éppen hogy csak átlépi, ezért érthetőségük korlátos. A különböző településeken a hangosbeszélők (közismert nevükön lármafák) a szirénáknál is ritkábban vannak elhelyezve, az a távolság, amelyről a bement szöveget még érteni lehet pedig töredéke a szirénák hatótávolságának. A mobil hangosbeszélők (rendőrségi, önkormányzati stb.) vagy járműre szerelt, vagy kézi (hordozható) változatban biztosítják a lakosság tájékoztatását. A mozgás és a háttérzaj ebben az esetben is lényegesen lerontja az érthetőségi küszöböt.

A fenti megoldások elemzése után megállapítható, hogy Magyarországon a lakossági riasztás rendszere korszerűtlen, és területi kiterjedésében sem teljes mértékben megoldott. A lakossági riasztási rendszer nem használja ki a modern távközlés adta műszaki lehetőségeket, sem a szolgáltatások jellegét, sem földrajzi kiterjedését tekintve. Ugyanakkor a mai távközlési hálózatok alkalmasak olyan szolgáltatások nyújtására (számos külföldi példa bizonyítja), amelyek biztosíthatják a kritikus területen tartózkodó emberek azonnali riasztását és tájékoztatását mobil és/vagy vezetékessé telefonon keresztül. Ennek többféle megoldása lehetséges:

1. A telefonközpont a riasztásban érintett körzetben gépi úton (automatikusan) felhívja az előfizető készülékét (mobil vagy vezetékessé) és egy előre beprogramozott hangbementést küld. Ez a hangbementés gyakorlatilag a riasztásba bevont valamennyi előfizető felé érvényesíthető, ami sok esetben nagyobb kör lehet, mint a fent ismertetett három „tradicionalis” megoldás összessége. Előnyei:
 - A hangbementés jellege számos módon kombinálható az előkészítettségtől, a pillanatnyi igénytől, és a riasztottak helyzetétől függően, és a riasztási területen tartózkodók jelentős része (ide értve a dolgozókat, kirándulókat, közlekedőket, zajos tevékenységet folytatókat, és az alvókat is) mobil- vagy vezetékessé telefonon nagy valószínűséggel elérhető.
 - A riasztást akár több nyelven is lehet közölni, ha az adott körzetben feltételezhetően sok külföldi állampolgár tartózkodik (pl. turistaközpontokban, nemzetközi kiállítások, konferenciák esetén), és ha erre a lehetőségre műszakilag is felkészítették a rendszert.
 - A bement információ korlátlan számban megismételhető akár automatikusan, akár a riasztott kezdeményezésére.

- A riasztások fogadását figyelve, a központba visszaérkező jelzések (pl. beemelés, tartásidő), lehetőséget adnak annak automatikus felmérésére, hogy a riasztást és a tájékoztatást hányan és milyen körzetekben hallgatták meg. Az így előállt adatok, információk nagymértékben elősegítenék a mentésben résztvevő szervezetek munkáját. (Például a körzetben tartózkodók száma megbecsülhető lenne.)
 - A riasztás után az érintettek, a riasztási üzenetben megadott számon azonnali (ingyenes) segítséget kérhetnek a körzetükben tartózkodó, és a mentésben résztvevő emberektől, amely kétségtelenül jótékony pszichikai hatású lehet, az őket ért első sokk után. Így elkerülhető a pánik, és az intézkedéseket szervezettebben lehet végrehajtani.
 - A riasztási terület felé haladó, mobil készülékkel rendelkezők számára a fennálló veszélyhelyzet előre jelezhető (a riasztási területet környező cellákban más jellegű riasztás, figyelem felhívás történhet). Ha az értesítés gépkocsiban utazó személyekhez jut el, a közlés azt is tartalmazhatja, hogy mely irányba kerüljenek, vagy saját érdekükben, esetleg tiltás miatt, mely irányokba ne haladjanak tovább.
2. A másik lehetőség szöveges üzenet (SMS), vagy mobil hálózaton cella broadcast üzenet (CBM) küldése a riasztási körzetben tartózkodók számára. Az SMS szolgáltatást ma már nemcsak a mobil, hanem a vezetékös hálózatokban is használják, azonban hozzá kell tenni, hogy az előfizetőknél levő vezetékös telefonok jelentős része ma még nem tud szöveges üzenetet fogadni. Ennek ellenére a vezetékös telefonra küldött SMS üzenet eljut az előfizetőhöz, mert a szolgáltatás ilyenkor a központ segítségével gépi úton felhívja az előfizető készülékét és automata hangbemondással közvetíti az üzenet szövegét. Előnyei:
- Süketek és nagyothallók is értesíthetők, mert a zsebükben lévő mobiltelefon rezgő üzemmódja lehetővé teszi számukra az üzenet érkezésének észlelését. Sok esetben a telefon fényjelzéseket is ad, amely további segítséget nyújt az észlelésben. (Lehet vásárolni olyan kis szerkezeteket, amelyek érzékelik a mágneses tér hirtelen megváltozását és saját fényforrás villogtatásával jelzik a hívást.)
 - A szöveges üzenet másik előnye abban rejlik, hogy a kapott üzenet a mobil készülék memóriájában vagy a SIM kártyán tárolódik, ezért az üzenet akkor is megnézhető, ha az előfizető valamilyen ok miatt nem veszi fel a telefont egy riasztási hívás esetén. (Az üzenethagyás nem mindig hatékony megoldás, mert az üzenet lehallgatását általában nem azonnal kezdeményezik az előfizetők, és még pénzbe is kerül).

Teendők az újfajta lakosságriasztási szolgáltatás bevezethetősége érdekében:

Egy újfajta a távközlési hálózatok szolgáltatásaira alapuló, veszélyhelyzeti riasztási rendszer bevezetéséhez és alkalmazásához – a hagyományos riasztási rendszerek korszerűsítése és meghagyása mellett – az alábbi lépéseket lehetne alkalmazni:

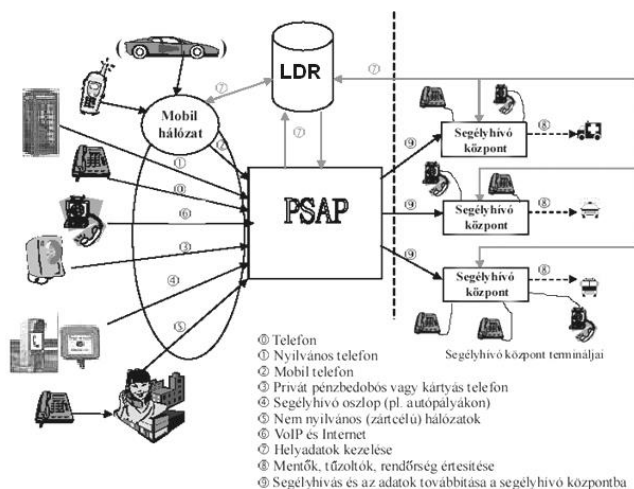
- a) Ki kell dolgozni a műszaki megoldások lehetőségeinek elvét, várható költségeit, és a bevezetés időigényét.
- b) Ki kell jelölni a riasztás rendszerének felügyeleti szerveit és központjait.
- c) A hazai lakosságriasztással foglalkozó jogszabályokat a fenti szempontok tekintetében módosítani kell, és figyelembe kell venni a riasztással foglalkozó ETSI ajánlásban megfogalmazott célokat és eszközöket.

Egységes európai segélyhívószám (112)

A 112 nemzetközi segélyhívószám alkalmazását és annak bevezetését az EU országaiban az Egyetemes szolgáltatási irányelv (Universal Service Directive 2002/22/EC) írja elő, ezért a direktíva a 2003. évi C. törvény az elektronikus hírközlésről egyik meghatározó alapidokumentuma. A segélyhívószám 2000-től működik országos szinten Magyarországon, a 112 segélyhívó központok kezelését a BM végzi. A segélyhívások általában a segélyhívás helyéhez legközelebb eső megyei rendőrkapitányságokra futnak be. A segélyhívások komplex kezelését nem támogatja összehangolt informatikai rendszer, mert ennek kiépítésére nem álltak rendelkezésre megfelelő anyagi eszközök. A központok üzemeltetésének személyi, tárgyi és anyagi feltételeit lényegében a Belügyminisztérium gazdálkodik ki saját költségvetéséből, állami támogatást külön erre a célra eddig nem kapott. Abban az esetben, ha valamelyik központban a nagyszámú hívás miatt (ez pl. tömegbaleset, robbanás stb. esetén gyakran előfordul) hívástorlódás lép fel, a segélyhívások várokozhatnak (sokszor több percig is), amíg nem lesz felszabadult fogadási kapacitás, más központba való átirányítás torlódás esetén nincs. A 112 nemzetközi segélyhívószám alkalmazására, és a segélyhívások kezelésének szabályozására több európai szintű ajánlás ad útmutatásokat. Az EU a 2005-ben végzett felmérései alapján kedvezőtlenül ítélte meg az egységes európai segélyhívószám bevezetésének és alkalmazásának elterjedését az EU országaiban, többek között hazánkban is. Ezért felhívta a tagországokat, hogy vizsgálják felül a rendszer országon belüli alkalmazásának körülményeit, és a kormányzatok készítsenek terveket és tegyenek erőfeszítéseket a segélyhívások kezelésével kapcsolatos előírások, ajánlások betartása érdekében.

A 112 hívásakor a mobil hálózat üzemeltetője nem végez sem előfizetői hitelesítést, sem készülék (IMEI) ellenőrzést, ezt nemzetközi szabályok írják elő. Ez azt jelenti, hogy a segélyhívó szám minden körülmények között működik, még akkor is, ha a mobil készülékben nincs SIM kártya, és/vagy ha a készülék

ki van tiltva a hálózathoz (például azért mert lopott). Az EHT előírja, hogy a 112 hívása ingyenes, a kapcsolat felépítésében résztvevő egyetlen távközlési szolgáltató sem kérhet a hívásért díjat (sem egymástól, sem a hívótól). Az Európai Bizottság 2003/558/EC ajánlása részletesen szabályozza a helyadatokkal kiegészített segélyhívások E112 (Enhanced 112) feldolgozásának és továbbításának elveit és szabályait az elektronikus hírközlési hálózatokban. Magyarországon a 112 hívásakor a segélyhívó központokban nem áll automatikus rendelkezésre a segélyhívás beérkezésekor helyinformáció, mert az alkalmazott távközlési rendszer alkalmatlan az európai előírások megvalósítására, az E112 bevezetésére. Magyarországon csak szigorú szabályozási környezet megalkotásával és jelentős anyagi ráfordítással valósíthatók meg korszerű segélyhívó informatikai rendszerek. A 2. ábrán az ETSI 002 180 ajánlása javasolt megoldást lehet látni. Az E112 hívásokat először a PSAP (Public Safety Answering Point) központi egység fogadja, amely automatikus jelzésszintű kapcsolatban áll az LDR (Location Data Retrieval) nevű, helyinformációkat kezelő és tároló egységgel. Az LDR vezérli az aktuális helyadatok lekérését abból a hálózathoz, ahonnan a segélyhívást kezdeményezték, majd az adatokat azonnal továbbítja a PSAP felé. A PSAP ezután a hívást az aktuális helyadatokkal együtt a segélyhívás helyéhez legközelebbi segélyhívó központba irányítja. A segélyhívó központok termináljain a térinformatikai rendszer segítségével azonnal megjelenik a hívó fél azonosítója („A” szám) és földrajzi helye. A megfelelő intézkedéshez szükséges további információkat a segélyhívó központban dolgozó diszpécser szóban tudakolja meg a segélykérőtől (amelyről felvétel is készül), majd az adatokat számítógépen rögzíti. Az információk ismeretében a diszpécsernek kell döntenie a további intézkedésekről, azaz ő fogja meghatározni, hogy az egységes informatikai rendszeren keresztül melyik szervezetet értesíti az eseményekről. A szervezetek mozgó, vagy fix helyű állomásai az informatikai rendszer segítségével azonnal lekérhetik a diszpécser által rögzített, valamint a PSAP-ból küldött információkat. Erre a Magyarországon alkalmazott TETRA rendszer maximálisan alkalmas. Minden esemény összes alapinformációja, valamint az intézkedések logikai és időbeli sorrendje az informatikai rendszerben logolódik, majd archiválásra kerül. Ez a megoldás támogatja az egyes esetek pontos rekonstrukcióját, ha valamilyen későbbi eljárás, intézkedés ezt indokoltá teszi (pl. bírósági eljárás, nyomozás, államvédelem stb.).



2. ábra. E112 szolgáltatás rendszerteknikai háttere az ETSI ajánlása alapján

Távközlési hálózatok együttműködése

Tételezzük fel, hogy valahol Magyarországon egy hatalmas erejű szélvihar következtében működésképtelenné válik az érintett területen található bázisállomások többsége (az antennákat leszaggatta a vihar). Az egyik állomás mégis üzemképes marad, és csak ez tud lefedettséget biztosítani a környéken. Az állomást az egyik mobilszolgáltató üzemelteti, ezért csak a saját hálózatának előfizetői tudnak hívásokat kezdeményezni. A körzetben tartózkodó többi előfizető (ha magyar) csak segélyhívó számokat tud hívni az épségben maradt bázisállomáson keresztül. A más szolgáltatókhoz tartozó előfizetők nem tudnak normál hívásokat kezdeményezni (például azért, hogy megnyugtassák hozzátartozóikat), ami az addig átélt események miatti stresszt csak tovább fokozza.

Mit lehet ilyenkor tenni?

- Keresni egy nyilvános telefonfülkét (ami több órán át is eltarthat), de az erős szél következtében leszakadt kábel miatt az sem működik.
- Minden arra haladó, mobiltelefonáló embert megállítani, és megkérdezni, hogy az ő telefonja működik-e, ha igen, kölcsönkérni a telefont.
- Keresni gyorsan egy nyitva tartó ügyfélszolgálatot, ahol kapható olyan SIM kártya, amely a működőképes bázisállomáshoz kapcsolódik. Ha az illető mobilkészüléke nem hálózat független, ez a megoldás sem jó.

A szarkasztikusnak tűnő válaszok reális helyzeteket írnak le, a helyzet megoldásán pedig komolyan el kellene gondolkozni. Egyik lehetséges megoldásnak tartom a következőt:

A működésképtelenné vált bázisállomások szolgáltatói értesítik a harmadik szolgáltatót az eseményekről. Tételezzük fel, hogy a három szolgáltató olyan szerződést kötött, hogy üzemzavar esetén kisegítik egymást, és ha korlátozott számban is, de lehetőséget adnak arra, hogy egymás előfizetőit kiszolgálják. A SIM kártyán ugyanis tárolva van az előfizető számára tiltott elérési hálózatok listája (Magyarországon a három szolgáltató között nincs roaming szerződés), ami eleve kizárja az előfizetőt a másik két szolgáltató hálózatához való hozzáféréstől. A működőképes bázisállomás szükségesetben ideiglenesen olyan információt sugároz, amely blokkolja a SIM kártyán található tiltólistát, azaz a telefon be tud jelentkezni az új hálózatba. Mivel a hálózathoz való kapcsolódáshoz szükséges az előfizetői azonosság hitelesítése, a kiszolgáló hálózat az IMSI alapján transferálja az előfizetői adatokat az előfizető honos hálózatába, ahol megtörténik a hitelesítés. A szolgáltatás biztosítása így a honos szolgáltató támogatásával és beleegyezésével történik, de a másik szolgáltató hálózatán keresztül. A díjazást pedig a szerződésben foglalt feltételek szerint rendezik. A szakszargonban a mobil kezdeményezésű hívás neve *Mobil Originated Call* (MOC), ezért a javasolt szolgáltatást *EMOC*-nak (Emergency MOC), azaz „veszélyhelyzeti mobil hívásnak” nevezném el (nem azonos a segélyhívással).

A fenti példa jól mutatja, hogy Magyarországon a távközlési hálózatok üzemeltetői válsághelyzetben nem működnek együtt, igaz erre semmilyen szabályozás nem kötelezi őket. Veszélyhelyzetekben a hálózatok összekapcsolásának lehetősége, így meghibásodás, torlódás esetén a forgalom egyik hálózatról a másikba való átirányítása és kezelése, csak jól koordinált hálózatmenedzsment rendszerek, hálózatfelügyelet támogatásával valósulhatna meg. Ezzel szemben magyar távközlési szolgáltatók hálózatfelügyeleti rendszerek egymástól függetlenül, elszigetelt módon működnek, ezek fizikai összekapcsolása sem műszakilag, sem szabályozási oldalról nincs kidolgozva, ezért válsághelyzetben csak adminisztratív megoldások állnak rendelkezésre (lejelentik a problémát az NHH-nak). Az ITU és az ANSI (American National Standard Institute) több szabványosítási projektet indított a hálózatok közötti együttműködés és összekapcsolás veszélyhelyzeti távközlést érintő problémáinak megoldására. A két testület a hálózatmenedzsment rendszerek ilyen célú együttműködésének megoldását a szabványosított TMN-X interfészen keresztül ajánlja. Ez az interfész nem ismeretlen a hálózatok közötti kommunikációban, azonban a veszélyhelyzeti alkalmazásokhoz szükséges alkalmazási protokollok alkalmazása még nem elterjedt.

Összefoglalás

Összegzőképpen megállapítható, hogy **Magyarországon a polgári lakosságot érintő veszélyhelyzeti kommunikáció – riasztás és segélykérés – korszerűtlen, nem felel meg a az európai unió és más nemzetközi elvárások-**

nak, ezért szükséges ezek minél előbbi korszerűsítése. Az is kijelenthető, hogy **a magyar hatályos jogszabályok nem biztosítják hatékonyan sem a felkészülést, sem a minősített időszaki feladatok elvégzéséhez szükséges operatív intézkedési mechanizmust.** Bizonyos jogszabályok ugyan részletesen előírják a területhez kapcsolódó feladatokat, azonban azok végrehajtásának módját és annak ellenőrzési rendszerét nem, és nem azonosítható a hatóságok szerepe és felelőssége sem. Megállapítható továbbá, hogy **Magyarország távközlési rendszerének és infrastruktúrájának felkészültsége – a szükséges mennyiségű tartalékok és a hálózatok veszélyhelyzeti együttműködésének hiányában – nem alkalmas a bekövetkező válságesemények hatékony kezelésére.**

A KÉRDÉS MÁR NEM AZ, HOGY A KATASZTRÓFA BEKÖVETKEZIK-E, A KÉRDÉS AZ, HOGY MIKOR? MEDDIG VÁRJUNK MÉG, HOGY AZ „ILLETÉKESEK” VÉGRE FELÉBREDJENEK!

MI, MÉRNÖKÖK KÉSZEN ÁLLUNK!

Pál Tamás

Lépéskényszer és lehetőség a közigazgatásban

Kényszerítő erők

A magyar közigazgatásnak egy elodázhatatlan változási (reform) folyamat fókuszpontjában kell állnia, amit egyszerre külső, és belső megújulási kényszer is indukál. Külső kényszerítő erőt egyrészt az Európai Unió Lisszaboni Stratégiájában foglalt célok – 2010-re Európának a világ legversenyképesebb, legdinamikusabban fejlődő, tudásalapú társadalmának kell lennie – megvalósítása, másrészt az ország külső adósságállománya finanszírozhatóságának biztosítása, versenyképességének növelése jelenti. Mindez az euró-övezethez való csatlakozás menetrendjét összefoglaló Konvergencia-program teljesítésében ölt testet. Magyarországon a közigazgatásra fordított kiadások 2004-ben a GDP 3,8%-át tették ki, amely nemcsak mind a EU régi 15 tagállamának átlagánál magasabb, hanem meghaladja a visegrádi országok átlagát is. Elsősorban a teljesítőképesség növelésére kell koncentrálni, mely a közszolgáltatások pénzügyi, és tranzakciós költségeinek mérséklését is eredményezi.

A belső kényszerként – összefüggésben az előzővel – az államháztartás helyzetéből következő feszes gazdálkodás, valamint a közigazgatás ügyfeleinek (állampolgárok, vállalkozások) igényei jelentkeznek.

Mindezek mellett viszont a 2007-től megnyíló európai uniós források óriási lehetőséget is jelentek a közigazgatás megújítására. Az Unió is felismerte, hogy a közigazgatás a gazdasági fejlődés gátját is jelentheti, ezért a támogatási célok között kitüntetett szerepet kap a közszolgáltatások minőségének javítása, az on-line lakossági szolgáltatások kialakulásának elősegítése. Egy ország versenyképességének javításához a fenntartható gazdasági növekedés biztosításához nélkülözhetetlen a hatékonyan működő, magas szintű közszolgáltatásokat nyújtó közigazgatás, ami már nemcsak a hazai gazdasági szereplők igényeit, hanem a nemzetközi vállalkozásokat képes kiszolgálni.

Olyan sajátos helyzetbe kerültünk, hogy a kényszer és a lehetőség egyszerre van jelen. Ezek a hajtóerők pedig remélhetőleg egy irányba, a hatékonyság, a teljesítőképesség növelése felé vezet(het)ik a magyar közigazgatást.

Fejlesztés esélye

Az Európai Unió következő, 2007-2013-as költségvetési ciklusában Magyarország számára jelentős pénzügyi források válnak elérhetővé. Hazánk fejlődését alapjaiban határozza meg, hogy a rendelkezésre álló 22,6 milliárd euró fejlesztési támogatás milyen hatékonysággal kerül felhasználásra. Ebben az esetben a hatékonyság nem csupán azt a közgazdasági fogalmat jelenti, hogy egységnyi ráfordítással minél nagyobb output kerüljön realizálásra, ha-

nem annak biztosítását is, hogy a megvalósuló programok hosszú távon fenntartható gazdasági, és társadalmi hasznot eredményezzenek. Ez pedig csak akkor valósulhat meg, ha a projektek összehangoltan, az egymást erősítő szinergikus hatásokat kihasználva kerülnek tervezésre, előkészítésre és végrehajtásra.

A fejlesztési források elnyerésének fontos előfeltétele az előzetes tervezés, a megfelelő intézményrendszer felállítása, annak érdekében, hogy a közpénzek felhasználása követhető, átlátható, és hatékony legyen. A 2007-2013 közötti időszakban Magyarország számára elérhető támogatások fogadására történő felkészülés jegyében, a Kormány a tervezési folyamat feladatait és felelősségi rendjét az Európa Terv (2007-2013.) kidolgozásának tartalmi és szervezeti kereteiről szóló 1076/2004. (VII.22.) Korm. határozatban rögzítette.

Az eddig elkészült valamennyi tervezési dokumentumban – a társadalmi vitára bocsátott Új Magyarország Fejlesztési Terv, operatív programok kivonatai – megfogalmazódott cél, az állami szerepvállalás minőségének javítása, a közigazgatás szolgáltatásainak fejlesztése és racionalizálása. A 1076/2004. (VII.22.) Korm. határozat értelmében a közigazgatás modernizálásával kapcsolatos tervezési feladatok a Miniszterelnöki Hivatal irányításával indultak el. Ugyanakkor még nyitott a leglényegesebb kérdés, hogy a közigazgatási szféra önmaga képes lesz-e arra, hogy az eddigiektől lényegesen eltérő szemlélettel közelítsen önnön problémájának megoldásához.

Mit kell(ene) tenni?

A közigazgatás korszerűsítése, és ennek a stratégiai tervekben való megjelenítése új megközelítést kíván, hiszen egyszerre kell áttörést elérni:

- a) a jogi szabályozásban,
- b) a működési folyamatok átalakításában, racionalizálásában,
- c) az irányítási, döntési és szervezeti rendszer korszerűsítésében,
- d) az informatikai infrastrukturális háttér kialakításában,
- e) valamint a humán erőforrás fejlesztésében.

A reformlépések tervezésekor mindenekelőtt a közigazgatással szemben támasztott elvárásokból kell kiindulni (ügyfelek igényei, gazdaságossági elvárások), majd a közigazgatás funkcióit, a közigazgatási folyamatokat, a vertikális és horizontális együttműködések lehetőségét, a szervezetfejlesztési, szervezetskorszerűsítési feladatokat szükséges áttekinteni. Erősíteni szükséges a jogi szabályozás színvonalát – elsősorban a jogszabály-előkészítést megalapozó hatáselemzések terén – az emberi erőforrások fejlesztését, valamint az e-közigazgatás elterjesztését. Egyszerűsíteni kell a közigazgatási ügyintézés folyamatát, hatékony ügymenetet támogató infrastrukturális fejlesztéseket kell

támogatni, ehhez az alapnyilvántartások fejlesztését (pl. személy- és lakcímnilvántartás, járműnyilvántartás), a hazai és uniós informatikai rendszerek között lévő adatkapcsolatok kiépítését kell megteremteni. A közigazgatás teljesítő-képessége jelentős mértékben a rendelkezésére álló személyi állománytól, és a szervezeti kultúrától függ. A közigazgatás reformja a köztisztviselők szemléletváltozását is megköveteli. Olyan kompetenciák fejlesztése válik szükségessé, mint a stratégiai gondolkodás, ügyfélorientáltság, vagy az egyéni teljesítmény növelése. Így érhető el, hogy a hivatali ügyintézés egyszerűbbé, érthetőbbé és áttekinthetőbbé váljon.

Ügyfelek elvárásai

2006 májusában a M-Á.S.T. Piac- és Közvéleménykutató Társaság kutatást végzett a magyar lakosság közigazgatási ügyintézéssel kapcsolatos attitűdjeinek feltárására⁴⁴. A kutatás eredményei szerint, egy magyar 18 éven felüli állampolgár 2005-ben átlagosan 1,6 ügyet intézett. Az ügyek 86%-a személyesen, egy hivatalban kezdődött, 10,2% indult levelezéssel, 3,4% telefonnal, míg mindössze 0,5% elektronikus formában. A válaszadók közül legtöbben az okmányirodával kerültek kapcsolatba. A megkérdezettek negyede intézett ügyet a Földhivatalban és az Adóhivatalban, ötöde az Illetékhivatallal, az önkormányzat adóosztályával a TB Egészségpénztárával és Nyugdíjpénztárával valamint a rendőrséggel került kapcsolatba. A legkevesebben a Vám- és Pénzügyőrséggel kerültek kapcsolatba, mindössze 3%.

A válaszadók véleménye szerint a hivatali ügyintézéshez a leginkább kitarásra, türelemre van szükség. Leginkább az ügyintézőkkel, a legkevésbé a költségekkel, a sorakerülésig tartó várakozási idővel és az ügyintézés egyszerűségével voltak elégedettek. Az ügyintézéssel szemben támasztott legfontosabb követelmény a korrupció mentesség, az ügyintézők szakértelme, és az ügy teljes elintézési ideje.

A kutatás alapján, az okmányirodába történő oda-vissza utazás átlagosan $49,1 \pm 1,6$ percet vett igénybe. A válaszadók 17%-nak egy óránál többre volt szüksége. Átlagos sorbanállási idő 36,9 perc volt.

A megkérdezettek 11,8%-a próbált már valamilyen közigazgatási ügyintézés során interneten információt szerezni vagy ügyet intézni. A legtöbben információt gyűjtöttek, de 48,9% ki is nyomtatott valamilyen nyomtatványt, 24,3% elektronikusan ki is töltött ilyet és 21,9% kért információt e-mailben. Az e-közigazgatás használói alapvetően két olyan területet látnak, ahol a teljes körű elektronikus ügyintézésre mihamarabb szükség lenne. Ezek az okmány-

⁴⁴ 2000 fős mintán végzett vizsgálat

irodai ügyek (77,8% említette a négy legfontosabb terület között) és az adózás (56,2%).

A vizsgálat következtetéseként levonható, hogy az ügyfelek nem tudják, hogy mely ügyeket mely közigazgatási szervnél intézhetik el, milyen feltételeknek kell megfelelniük, mivel a közigazgatás nem kellőképpen átlátható. Továbbá jelentős probléma, hogy hazánk különböző településen lakó emberek rendkívül eltérő színvonalon jutnak hozzá a közigazgatási szolgáltatásokhoz. Az állampolgárok szemszögéből tekintve szintén nehézséget jelent a hivatali nyitvatartási, ügyfélfogadási időhöz kötött ügyintézés. A hivatalokban csak munkaidőben lehet ügyet intézni, mert munkaidőn kívül csak kevés közintézmény tart nyitva, és akkor is csak általában plusz 1 órát. 2002-ben az államigazgatási szervek 91 %-ánál nem volt olyan ügyfélfogadási időszak, amelyben a rendes munkaidőn túl is lehetett ügyeket intézni. A közigazgatási ügyek intézéséhez rendszerint szabadságot kell kivenni.

A megfogalmazott igények világosak, az ügyfelek gyorsan, egyszerűen akarnak ügyeket intézni. Ennek megvalósítása érdekében kétirányú fejlesztést kell megvalósítani, amely egyrészt átfogja a személyes megjelenéssel járó ügyintézési formák jobb kialakítását, másrészt kihasználva az informatika nyújtotta előnyöket, az elektronikus közigazgatási szolgáltatások elterjesztését biztosítja.

Az elektronikus közigazgatás fejlesztése

A közzsféra jelenleg egymástól elszigetelt rendszerek, illetve redundáns folyamatokat fenntartó intézmények labirintusaként működik, ezért strukturális átalakításra szorul. A korszerűsítés egyik fő eleme és eszköze az elektronikus közigazgatás fejlesztése, amely nemcsak alapfeltétele a központi és területi államigazgatási (részben önkormányzati) reformnak, hanem annak mozgatórugójává is válhat. Az e-kormányzati eszközök és módszerek alkalmazása révén lehetőség nyílik egy modern állami szerepvállalás kiteljesítésére, az állam szolgáltató szerepének fejlesztésére. Az informatikai fejlesztésekkel nemcsak az ügyfél és hatóság között nyílik kommunikációs csatorna, hanem közigazgatás belső folyamatai is megújulhatnak.

2003-2005 között az elektronikus kormányzás középtávú stratégiájának meghatározását, a Magyar Információs Stratégia és az E-Kormányzat 2005 Elektronikus Kormányzat Stratégia és Programterv tartalmazta, melyet a Kormány a 1126/2003. (XII. 12.) számú Korm. határozattal fogadott el. A megfogalmazott célokat az Informatikai és Hírközlési Minisztérium költségvetése, az ágazati intézmények költségvetése, valamint az I. Nemzeti Fejlesztési Terv Gazdasági Versenyképesség Operatív Programjából finanszírozták. E három

forrásból, 2003 és 2005 között összesen mintegy 300 milliárd forint került felhasználásra.

Az elért eredmények leginkább abban mutatkoznak, hogy hazánk jelentős előrelépést tett az eEurope2005 akcióprogramban meghatározott 20 legkeresettebb közszolgáltatás on-line elérhetősége terén, amely nálunk 27 közigazgatási ügyre bővült. A 27 elektronikus közszolgáltatásnak a meghatározott elektronikus szolgáltatási szinten történő megvalósítását, a közigazgatás korszerűsítését szolgáló aktuális e-kormányzati feladatokról szóló 1044/2005. (V. 11.) Korm. határozat rendelte el. Az általános követelmény a teljes körű elektronikus tájékoztatás megvalósítása volt – amely az EU mérési módszere szerinti 1. szintnek felel meg –, a kiemelt prioritású ügyeknél elvárt legalább a formanyomtatványok letölthetőségét jelentette (2. szint). A háttérrendszerek technikai fejlettségétől, és a már meglévő vagy fejlesztés alatt álló szolgáltatások meglététől függően több közszolgáltatás esetében reális cél volt a 3. szint elérése, amely már az ügyiratok és dokumentumok kétirányú elektronikus továbbításának lehetőségét is magában foglalta. Bizonyos jól működő szolgáltatások esetében a háttérrendszer fejlettsége a későbbiekben lehetővé teszi – a jogszabályi feltételek biztosítása után – a 4. szint (teljes körű elektronikus ügyintézés) elérését is.

2005 végén a 27 szolgáltatásból 20 on-line is elérhetővé vált, míg a letölthető űrlapok, formanyomtatványok száma eléri a kétszázat. Ezzel az „EU 20 szolgáltatás” aggregált kidolgozottságának mértéke – amely a 2004. október 15-én 46 %-os szintet mutatott –, 2005. december 15-én már meghaladta a 80 %-os teljesítési szintet. Ezen mutatószámok tekintetében az európai uniós összehasonlításban 2005. év végére a tagországok rangsorában hazánk a középmezőny elejére került.

A továbbiakban a kormányzati informatikai fejlesztéseknek nem egyszerűen a különböző döntéshozatali szintekhez való igazodást kell támogatniuk, hanem elő kell mozdítaniuk a szervezeti racionalizálást, integrációt. A jövőben komplex és integrált közigazgatási rendszerekre van szükség, melyekkel egyszerűsíthető a közigazgatási ügyintézés folyamata. Nélkülözhetetlen a hazai és uniós informatikai rendszerek között lévő adatkapcsolatokat teljes kiépítése, összehangolása, valamint a hálózati biztonság megteremtése, hiszen ezáltal lesznek a szolgáltatások megbízhatóak, folyamatosan elérhetőek és biztonságosak. A hangsúlyt a folyamatok integrálására kell helyezni.

A fejlesztés alapját azok a közcélú adatbázisok, alapnyilvántartások – személyi adat- és lakcímnnyilvántartás, személyazonosító igazolvány nyilvántartás, lakcímgigazolvány rendszer; Anyakönyvi Szolgáltató alrendszer; tartózkodási

és letelepedési engedély nyilvántartás; országos járműnyilvántartás stb. – szolgáltató képességének a növelése kell, hogy jelentse, melyek az egész ország működésének alapját képezik, ezzel jelentősen meghatározzák a közigazgatás működésének szakszerűségét, hatékonyságát. Kiemelt jelentőségű, hogy minél többen hozzáférjenek a szolgáltatásokhoz. E cél érdekében az elektronikus távközlés korszerű lehetőségeinek, valamint az internethez történő hozzáférés minden módjának támogatása mellett figyelmet kell fordítani a közigazgatás-szervezésben rejlő lehetőségekre.

Annak ellenére, hogy az e-közigazgatás jogi szabályozásában történt előrelépés az elmúlt időszakban (pl. a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.); az elektronikus ügyintézés részletes szabályairól szóló 193/2005. (IX. 22.) Korm. rendelet; IHM rendeletek stb.), az eddigi tapasztalatok alapján a jogszabályok átdolgozásra és kiegészítésre szorulnak.

A közigazgatási ügyek intézésének teljes körű és magasabb szintű megvalósítása az ügyek számossága – több mint 2000 közigazgatási ügytípus – és a közigazgatási intézmények háttér-rendszereinek eltérő fejlettsége miatt csak fokozatosan valósítható meg, melynek során azoknak a szolgáltatásoknak a megvalósítása kap nagyobb prioritást, amelyeket az állampolgárok a leggyakrabban vesznek igénybe.

Az információáramlás hatékonyabbá tétele, az ügymenetet támogató infrastrukturális fejlesztések végrehajtása azért is fontos, mert a hazai állami intézményeknek az európai vérkeringés részeként rendszeres horizontális adatszolgáltatást is kell végeznie mind a többi tagállami társintézmény, mind az Unió központi intézményei részére.

Szolgáltató központok létrehozása

Az utóbbi néhány évben hangoztatott legfontosabb célkitűzés az volt, hogy közelebb kell vinni az állampolgárokhoz az egyes igazgatási, hatósági funkciókat szolgáltatásokat, viszont a hangzatos szövegek után, a számottevő eredmények elmaradtak. A közigazgatásban az ügyintézés menete mindig az adminisztráció igényei alapján került meghatározásra, így az ügyfelek szempontjai általában a háttérbe szorultak. Az ügyfélközpontú közigazgatást az elektronikus közigazgatás fejlesztésén, jogi akadálymentesítésén túl, a személyes megjelenéshez kötött szolgáltatások korszerűbb kialakítása segíti elő. Ehhez viszont át kell alakítani a központi, területi, regionális, és helyi közigazgatási szintek funkcióit, a közigazgatás feladatait. Újra kell szervezni a közigazgatási folyamatokat, a vertikális és horizontális együttműködések lehetőségét, a szervezetfejlesztési, szervezatkorszerűsítési feladatokat.

Az állam lokális szervei a módosított statisztikai kistérségi rendszerben című 2004-ben készült felmérés szerint⁴⁵, a kistérségenként vizsgált 15 intézmény (okmányiroda, városi gyámhivatal, építésigazgatási hatóság, szociális igazgatási hatóság, munkaügyi kirendeltség, APEH kirendeltség, ANT SZ városi intézet, körzeti földhivatal, rendőrkapitányság, hivatásos tűzoltó parancsnokság, polgári védelmi körzeti parancsnokság, körzeti vámhivatal, városi bíróság, városi ügyészség, közjegyzőség) közül a 168 kistérség 49 %-a rendelkezett 12-15 intézménnyel, 16 %-a 9-12 intézménnyel és a 25 %-a 5-8 intézménnyel. A továbbfejlesztés iránya ezekben az intézményhiányos kistérségekben nem lehet a jelenlegi az intézményhálózat bővítése, hanem sokkal célszerűbbnek tűnik a közigazgatási szolgáltatásokat integrált szervezeti modellben közelebb vinni az állampolgárokhoz. Elsősorban a meglévő szervezeti és humán bázisokon, valamint racionalizáló szervezeti összevonással teljes körűvé tehető az igazgatási szervek jelenléte valamennyi kistérségben, és megvalósítható az a hosszú évtizedek óta csak tervezett, de ténylegesen végre nem hajtott modernizációs reformlépés, hogy ne az állampolgárok járják a hivatalokat, hanem az ügyintézők várják őket egy helyen, s részükre minőségi közszolgáltatást biztosítson az állam.

Jelenleg számos közigazgatási szerv tart fenn – esetenként nem kis létszámú – ügyfélszolgálatot, tanácsadó szolgálatot, azonban ezek a szolgáltatások nem állnak össze rendszerré. Az elaprózott, jelentős térségi különbségeket mutató államigazgatási szervek ügyfélszolgálati egységei nem képesek hatékonyan kielégíteni az állampolgárok és az üzleti szféra igényeit. Az ügyfelek ideje ugyanis jelentősen felértékelődött. Nagyon sokan pénzben kifejezhető veszteségeket szenvednek, ha túl sok időt fordítanak a hivatalos ügyeik elintézésére. Az állampolgároknak gyakran nem csak egy ügyet kell elintézniük, hanem egy-egy esemény kapcsán több kapcsolódó intézménnyel is keletkezik. A hasonló vagy összefüggő ügyek államigazgatási eljárásai jelenleg nincsenek összehangolva. A közigazgatási eljárások elveikben sokszor nagyon hasonlítanak egymásra, de ez a hasonlóság messze nem tükröződik a jelenlegi eljárási gyakorlaton.

Nem történt meg a belső folyamatok újrászervezése, nem alakították ki a szabályozott ügymenetet. Az ügyfélszolgálati irodák az esetek többségében egy adott ügyben tájékoztatják az ügyfelet, illetve fogadják és ellenőrzik a beadványokat.

⁴⁵ Dr. Szigeti Ernő: *az állam lokális szervei a módosított statisztikai kistérségi rendszerben (gyorsvizsgálat)*, MKI

A térségi, intézményi összefogás, az összehangolt szakmai munka, a szellemi és anyagi erőforrások koncentrálása nagymértékben elősegítené a magasabb színvonalú szolgáltatások biztosítását. A közigazgatás átalakításának fontos elemét jelentheti, ha a különböző közigazgatási szervek közös szolgáltató egységeket hoznak létre, amelyekben az informatikai alkalmazások előnyeiket kihasználva, egy helyen, a lehető legtöbb ügyet el lehet intézni. Az államigazgatási szervek közös ügyfélszolgálatát, a közigazgatási reform egyik központi elemének tekintett térségi összefogás ideális színterén, azaz kistérségi szinten kell létrehozni.

Integrált ügyintézési szolgáltatást kell megvalósítani, melynek alapját azok a helyi, körzeti államigazgatási szervek képezik, és továbbfejlesztésükkel, illetve megerősítésükkel elérhetőségük jelentős mértékben javul. Így az állampolgároknak ügyintézés esetén csak egyetlen helyre kell befáradniuk, a háttér munkát a szakhatóságok végzik el. A különböző közigazgatási szervezeteknek nem kell létrehozniuk saját ügyfélszolgálati egységeket.

A térségi közigazgatási szolgáltató irodaközpontok megteremthetik a területi közigazgatás integrálásának informatikai, illetve szervezeti feltételeit, s ezzel együtt megalapozhatják az erősen széttagolt dekoncentrált szervezeti struktúra racionalizálását. További lépésként elősegíthetik az önkormányzati és államigazgatási feladatok szisztematikus szétválasztását, ami a finanszírozásban is egyértelműbb helyzetet teremthet. A szolgáltató központokba elsősorban az ügyfelekkel rendszeres kapcsolatban álló közigazgatási szervek képviselőit célszerű telepíteni. Első helyen az okmányirodák által intézett ügyek (személyi igazolvány, lakcím igazolvány, vezetői engedély, útlevél, vállalkozói igazolvány, pakolási igazolvány, gépjármű ügyintézés, anyakönyvi ügyek) szerepelhetnek, de célszerű az adóügyeket, az idegenrendészeti ügyeket, a földhivatali ügyintézés, a munkaügyeket bevonni ebbe a szervezetbe.

A közigazgatási ügyintézés és ügyfélszolgálat igénybevétele mellett az ügyfelek a közmű-szolgáltató vállalatokat (gázművek, elektromos művek, víz és csatornázási művek, stb.) keresik fel a leggyakrabban, tehát ezek ügyfélszolgálatait is célszerű az „Irodaközpont”-ba telepíteni. Az intézendő feladatok köre mindezekén túl a közüzemi szolgáltatásokhoz kapcsolódó ügyekkel is bővíthet. Növeli az ügyintézés koncentrációját, ha mindezen szervezetek mellett egyes szolgáltatók is (biztosító, közjegyző, ügyvéd, Internet szolgáltató, stb.) megjelenének a helyszínen kínált szolgáltatásaikkal.

A szolgáltató központok működésének további komfortosságát növeli pl. posta, call center, ügyfélirányítás, ATM automata, POS terminál telepítése is, melyek lényegesen hozzájárulhatnak az ügyfelek egy helyen történő komplex kiszolgálásához.

Az ügyfélközpontú közigazgatási ügyintézés kialakítása során át kell alakítani az ügyviteli eljárásokat, ami önmagában sem egyszerű feladat, de ebben az esetben még a hivatali szempontok prioritását is át kell engedni az ügyfelek részére. Korszerű informatikai eszközrendszer teljes körű felhasználásával, automatizáltan, és nyomon követhető ügyintézés valósítható meg. A közigazgatási ügyek elektronikus feldolgozása jelentősen javítja majd azok szabályozottságát, mert a programozott ügyintézés, vagy döntéshozatali eljárás kidolgozása során sokkal több részletre kell figyelemmel lenni, mint egy korábban nem modellezett, elképzeléseken alapuló szabályozásnál.

Természetesen nem lehet cél, hogy az ide telepített kirendeltségeken keresztül az összes ügyet teljes terjedelmében el lehessen intézni, mert túlságosan nagy infrastruktúrára, létszámra és ügyintézési időre lenne szükség. A legfontosabb, hogy megteremtődjön a feltétele az ügyfelek személyes megjelenéséhez kötődő összes ügyintézési elem elvégzésének, azaz a kérelem benyújtásának, a személy azonosságának ellenőrzésének, az ügyfél által bemutatott okmányok meglétének és hitelességének igazolásának, valamint az eljáráshoz kötődő díjak és/vagy illetékek kifizetésének. Ezek a feladatok tipikusan a „Front Office” funkcióknak felelnek meg, melyek után már az ügyfél jelenléte nélkül, az illetékes közigazgatási szerv székhelyén a háttérben (Back Office) kerülnek elintézésre az ügyek, melyek végeredménye (pl. határozat) általában postai kézbesítéssel kerül vissza az ügyfélhez.

Az ügyfélszolgálatok a hivatalok és a szolgáltatók lokális informatikai hálózatának kiterjesztésével és megfelelő felkészültségű ügyintézők delegálásával egyszerűen megvalósíthatók.

A szolgáltató központok várható előnyei:

- külön válik az ügyfél jelenlétét kívánó ügyrész a további ügyintézésről, ezáltal specifikálhatóbbá válik az ügyintézés folyamata;
- a hasonló ügyek Front Office része összevonásra kerülhet, így egy ügyintézői ablaknál egy időben több ügy is indítható;
- több ügy intézése esetén a személy azonosságának igazolása és az azonosító adatok rögzítése csak egyszer történik meg;
- az illetékek és díjak befizetése a helyszínen történhet;
- az eddigi ügymenetek korszerűsítését, logikusabb megoldását ösztönzi;
- a kialakuló azonos ügyfélszolgálati metodika egyszerűsíti és közérthetőbbé teszi a bürokráciát.

Prognosztizálható nehézségek

Az új ügymenetek megszervezésekor az ügyintézők feladatainak növekedését a folyamatok racionalizálásával és egyszerűsítésével célszerű kompenzálni,

de valószínű ez minden esetben nem oldható meg. Várhatóan mindez a jelenlegi ügyfelekkel foglalkozó köztisztviselői állomány kisebb-nagyobb ellenállásába fog ütközni. Az ügyfél szempontjából az a legcélszerűbb, ha a különböző ügyeit egyetlen ügyintézőnél tudja elintéztetni, ehhez viszont univerzális ügyintézők és integrált informatikai rendszerek szükségesek, melyhez a feltételek nem biztosítottak.

A szolgáltató központ koncepció esetén fennálló legjelentősebb problémát, hogy a megyeszékhelyeken, illetve kistérségi székhely településeken élők könnyebben, míg más települések lakói nehezebben érik el a közigazgatási szolgáltatásokat, ügyfélszolgálati pontok, terminálok hálózatával lehet csökkenteni. A településeken telepített terminál pontokon, megfelelően képzett ügyintézők segítségével komplex felvilágosítási, tájékoztatási közvetítői feladatok láthatók el, és megindíthatóvá válik az ügyintézés. Ügyindítás esetében az utazás megtakarítható, továbbá nem az ügyfélnek kellene kitalálnia, hogy problémájával, kérdésével hová forduljon, ezt a „közvetítő” megmondhatja, a kérdéseire a válaszokat beszerezheti. Bonyolultabb ügyek esetében pontosan megmondhatja, mikor, hová kell az ügyfélnek fordulnia. Ezek az ügyfélszolgálati pontokat össze lehet hangolni a teleházak rendszerével.

Ezáltal újabb csatorna nyílna az ügyfél és az illetékes állami vagy önkormányzati szerv között.

Ugyancsak az információhoz jutást segíti az egész országot átfogó Kormányzati Ügyféltájékoztató Központ (KÜK), melyet a közigazgatási tevékenység színvonalának javításához, a közigazgatási szervek szolgáltatásainak egységesítéséhez, együttműködésének javításához szükséges feladatokról szóló 1101/2005. (X. 25.) Korm. határozatban foglaltak szerint azért hoztak létre, hogy az állampolgárnak, az ügyfélnek minden egyes ügynél ne kelljen külön megtanulnia, hogy miként juthat a szükséges információhoz. A KÜK együttműködve a közigazgatási szervek ügyfélszolgálatával, egy helyről történő összehangolt tájékoztatást képes nyújtani.

ÖSSZEFOGLALÁS

A közigazgatás fejlesztésének középpontjába az állampolgárok, és a gazdaságkodó szervezetek igényeit és elvárásait kell helyezni, valamint párhuzamoságoktól mentes, költséghatékony, ésszerű ügyintéризést kell megvalósítani. Az állampolgároknak lehetőséget kell teremteni, hogy mind személyesen, mind pedig elektronikus úton intézhessék ügyeiket. Ebben kiemelkedő szerep hárul a különböző közigazgatási szervek közötti együttműködésre. Az ügyfélnek minden egyes ügynél ne kelljen külön megtanulnia, hogy miként juthat a szük-

séges információhoz, hanem csak az ügyintézés módját (személyes, vagy elektronikus) kelljen kiválasztania, és ennek megfelelően csak egy irodát, vagy egy honlapot kelljen csak felkeresnie. Nem az ügyfélnek kell idomulnia a hatósági struktúrához, hanem a hatóságoknak kell biztosítaniuk az ügyek, problémák megoldását az állampolgárnak.

A fent említett fejlesztések hiányában a gyenge hatásfokú közigazgatási működés konzerválódik, a közszolgáltatások színvonala tovább romlik az EU tagországok átlagához és a magánszféra szolgáltatásaihoz képest, amely az állampolgárok elégedetlenségének növelése mellett, az üzleti szférát, hazánk globális versenyhelyzetét is kedvezőtlenül érintheti.

Felhasznált irodalom

Dr. Dudás Ferenc: A nemzeti közigazgatás versenyképessége a személyi állomány, valamint a működés továbbfejlesztése tükrében, különös tekintettel az EU-s követelményekre (III. rész); Magyar Közigazgatás LIV. évf. 9. szám

Dr. Dudás Ferenc: Közigazgatásfejlesztési tendenciák a luxemburgi (miniszteri) tanácskozás tükrében III.; Magyar Közigazgatás LV. Évf. 11. szám

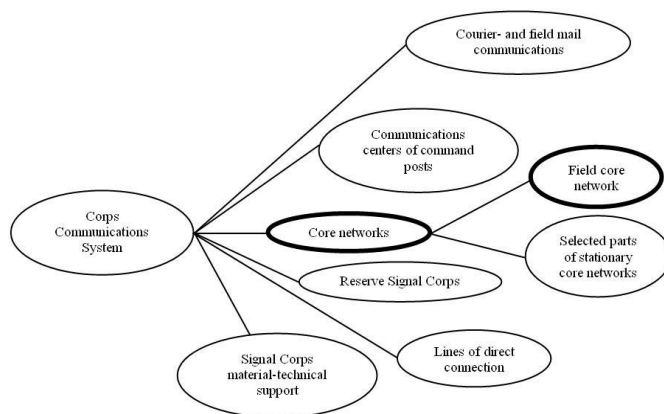
Dr. Szigeti Ernő: az állam lokális szervei a módosított statisztikai kistérségi rendszerben (gyorsvizsgálat), MKI

Balázs Pándi

Problems of the Core Communications Network

1. Definition of the field communications system

The operations of the Hungarian Defence Forces, and the quality of commanding troops, is largely influenced and its operation determined by the communications of the commanding levels, which especially in at the time of operations is realized by the complex application of the field communications system. This communications network facilitates communications and information exchange, between communications centers and users, independently of whether these are persons or end-point devices. This system should be considered as a subsystem of the weapon control system, which has been set up according to a standard concept and plan (communications plan). It consists of interconnected communications centers of different purposes, and the communications lines which connect them. It facilitates the exchange of information, and provides the terms of communications for the operation of the different command systems, including the personnel operating it. The core field communications network is the part of the mechanized corps, which consist of basic communications nodes and the communications lines that connect them, and provides the terms of communications for two or more levels of command (see the Figure below).



This means, that the command posts of the mechanized corps, and its subordinate combined arms, arms, and platoon units (primary and rear command posts), communicate through this network.

2. The command system of military communications and its characteristic problems

The command, control and maneuvering ability of the operation of the core communications network is unable to follow quickly changing situations, and is only able to adapt slowly to these. Commanding is mainly realized within hierarchically structured command system of the communications network, where the chief communication officers of military units coordinate the operations of communications sub-units of subordinate units through the available direct connections, service channels, with the help of operational-technical communications administration.

The professional leadership of the core communications network, is the duty of the chief communication officer of the mechanised corps, who has to provide all necessary information for the commander and officers of the communications unit installing the network, in order that the installation, establishment, and operation of the core communications network is provided for the time of the operations. The chief communication officers do their work based upon their professional experiences, however this is not supported by computer equipment and software as it would be normally expected in our age. For designing the communications networks' set up and layout on the field the special services do not currently have required software, geographical information systems, and designing programs, which could help in designing the connections, modelling the terrain or the operation of the network. The quantity and quality of computer equipment required to operate these kinds of software packages is also not provided for the communications services.

The installation of the basic communications centres can be described in terms of the collection of appropriate norms. For example, the installation of a communications centre, by a communications station operating with complete personnel, normally requires 150 minutes⁴⁶. If maneuvers or relocations are required in order to adapt to the dynamics of the operation, this can be achieved by using reserve units or by the relocation of basic communications centers already functioning in the system.

After setting up the communications system the primary task of the operational-technical units is the continuous monitoring, logging of the channels, and in case of failure their recovery, or leading the planning and execution of the recovery maneuvers. The core field communications network, in this sense is unable to electronically provide information about the incoming and outgoing channels at a basic communications centre, to the communications ad-

⁴⁶ Collection of standards for evaluating the special training of communications officers (publication of the Hungarian Peoples' Army Communications Command 1985. Print.no.: 108/105) page 108

ministration services. The remote administration does not function according to the standards of other NATO member countries.

The core field communications network can not be connected to the permanent public, some private and special networks because of their high level of digitalization. The situation is the same with the NATO Integrated Communication System and the field (tactical) communications systems of NATO member countries. In a multinational environment the simultaneous use of both of these networks is crucial for commanding troops. The operation of devices using analogue technology is complicated, and the time to train the administrating personnel is too long. Considering that the compulsory enlistment has been ended, training military units can be difficult be even at training centers.

The elements of the core communications network are technologically out dated, most of these are on the technological level of the year 1960-70 (or before), some them still use vacuum tube technology, and is no longer capable to compete with the services provided by modern telecommunications devices. The cost of maintaining these is very high. Their industrial renovation has been held off for years, due to its high costs and the closing of the manufacturing companies. The required materials for repairing the systems are hard to acquire, at some devices no longer possible. The lack of funds for acquiring materials for maintenance, and cease of production of the required parts for some devices, causes further difficulties in maintaining of the system. The probability of failure is high. The devices are not interchangeable because of their diversity. Block replacements can not be made, because of the lack of replacement units. Large quantities of repair materials are need for maintaining operability. Fast and modern panel replacements are not possible with the current equipment. The time and number of instruments required for the repairs is high. For a large number of devices, the repair is no longer possible. Among the operational radio-relay stations of the core field communications network, although the R-414 station is considerably modern, however it is not a device that provides channels according to the ITU⁴⁷ (previously CCITT⁴⁸) recommendations.

There has been an increasing need for commanding troops, to apply digital services on a tactical level, as well as:

- transfer of multimedia information,
- use of services provided by digital networks,
- decreasing paper-based information exchange in the process of decision-support, and decision making,
- fast and authenticated data transfer,

⁴⁷ ITU: International Telecommunication Union

⁴⁸ CCITT: Comité Consultatif International de Téléphone et Télégraphie

- operating a military messaging system (MMHS)⁴⁹, which is a basic requirement in the modern NATO systems.

3. Steps toward solving the problems

The core field communications networks of modern armies is such a digital grid system, that provides modern communications facilities for the commanders and staff taking part in commanding troops, and at the same time its' modern network management subsystem makes it possible for the decision-supporters and decision-makers to optimally use the available resources⁵⁰ at any time, in any situation, especially when rapid recovery is needed from damage caused by the enemy forces. The current troop commanding routines, exactly because of the high amount and high speed of information transfer, need to use a wide range of computer devices. Therefore the core field communications network is inconceivable without a technical subsystem that supports the special feature of network management of ensuring optimal use of resources, based upon a **new mathematical model**.

The previous studies I have made on this topic, show that this field is has not been investigated so far. All off these circumstances require the scientific overview, study and elaboration of the “automated” resource management of the field communications system, after which a recommendations can be made about the creation of a new subsystem based on mathematical and computer sciences.

4. Summary

In order to command the troops, the core field communications network provides communications infrastructure between the superior officers, the subordinate units, the combined arms reserve units and the cooperating troops, for the mechanized corps and its subordinate units. The communications devices comprising the basic communications centers use analogue technology, their telephone centers use manual switching, the workload on them is high. The channel-capacity of the network is small, its' maneuvering abilities are weak, and the planning of such maneuvers at the time of the operations require long and precise planning and a great deal of professional experience. The vehicles supporting the communications command system only provide work places operational-technical services, equipment for electronically monitoring the state of the channels, graphical displays of the conditions of the channels is not available for the services. The small number of manually switched service

⁴⁹MMHS: Military Message Handling System

⁵⁰ communications capacities, material-technical resources and human resources

channels does not allow the fast and flexible operative administration of the network, and even these are often used up for coordination of the operation. The designing and organization of the communications system requires a great deal of manual work (working with maps, drafts, plans, orders, etc.), and a substantial amount of time. The development of a technical subsystem supporting this special feature of network management based on a **new mathematical model** could be one of the steps towards solving these problems.

Bibliography:

- [1] Fekete, Karoly: Evolving possibilities of the strategic military networks, „Communication 2003” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86229 6 2, 15th October 2003
- [2] Hamar, Sándor: A katonai híradás fejlődésének és fejlesztésének lehetséges útjai, „Communication 2002” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 86229 2 X, 30th October 2002
- [3] Kozák, Miklós: A híradás alapvető fogalmai, workbook, Zrínyi Miklós Military Academy, Budapest, 1994
- [4] Rajnai, Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO tagországok kommunikációs rendszereinek tükrében, PhD dissertation, Zrínyi Miklós National Defence University, Budapest, 2001.
- [5] Somos, András PhD: A katonai kommunikáció és a hírközlés felkészítésének viszonya, International professional academic conference, Zrínyi Miklós National Defence University, Budapest, ISBN 963 00 8819 3, 28th November 2001

Szöllősi Sándor okl. mk. őrnagy

A magyar katonai híradás perspektívái

A Magyar Honvédség szervezeti és technikai átalakítása megkívánja valamennyi szóba jöhető információtovábbítási eljárás és eszköz számbavételét a legjobb megoldások kiválasztása érdekében. A tervezett rendszerek elsősorban az URH és a (földfelszíni) mikrohullámú összeköttetéseket részesítik előnyben. A tervezett RH megoldások inkább a „legyen még ilyen is, hátha kell” kategóriába esnek, véleményem szerint – más megoldásokkal egyetemben – nem kapnak kellő hangsúlyt. A lehetőségek áttekintése előtt még meg kell vizsgálni a szóba jöhető alkalmazási környezetet és a várható feladatokat.

A jelenlegi katonaföldrajzi és biztonságpolitikai kérdéseket áttekintve – és ez a doktrínákban is markánsan megjelenik – Magyarország jelenleg (és várhatóan a közeljövőben sem lesz) nincs közvetlen nyílt katonai támadásnak kitéve, annak veszélye nem fenyegeti. Ezzel szemben terroristatámadás lehetősége nem kizárható, egyfajta „üzenőfal” lehetünk katonai és politikai szövetségeseink irányába. Ez különösen azért igaz, mert az európai közös határvonal pillanatnyilag hazánk keleti, dél-délkeleti peremére húzódik át. Ezen a vonalon át jelentős migrációs tevékenység tapasztalható, mely esetenként elősegítheti a terrorizmus irányába hajló, vagy eleve terrorista személyek beszivárgását. Az ország tranzit jellege a korábbi évtizedekhez képest is jelentősen erősödött, sok esetben a bűnözést is elősegítve (pld. kábítószer-, hasadóanyag-csempészet, stb.). Mindezen feladatok megoldására a jelenlegi BM szervezetek jól felkészültek, katonai vonatkozása látszólag nincs. Mégis tovább kell tekinteni, hogy van-e olyan szituáció, amikor a katonára (is) szükség van. Alapesetben természetesen a természeti katasztrófák felszámolásában való aktív közreműködés jut az eszünkbe, melyre a közelmúltban is volt több példa. A másik, mely esetlegesen nagyobb létszámú erőket és technikai eszközparkot igényelhet, egy nagyobb tömeges közúti, vasúti katasztrófa, vagy ipari katasztrófa, esetleg ezek kombinációi. Ilyen jellegű helyzetet okozhat szélsőséges időjárás, ill. földrengés is. Megítélésem szerint ezen „békehelyzetekben” szükség van a katonákra, mert az erre szakosodott erők emberi és technikai erőforrásai végesek, segítség nélkül nem képesek – csak az áldozatok számának növekedése mellett – önállóan a hatások következményeit felszámolni.

A szándékosan okozott katasztrófák (pld. veszélyes anyagot termelő üzemek, gyárak felrobbantása, atomerőmű-katasztrófa előidézése, vízerőmű, víztározók gátjainak felrobbantása, vegyi- és biológiai szennyezések, energiaellátó rendszerek tönkretétele, távközlési hálózatok kommunikációjának megszüntetése, stb.) adott esetben olyan nagyságrendű és területű lehet, hogy csak a honvédség bevonásával van esély a következmények enyhítésére, ill. felszámolására.

A továbbiakban vizsgáljuk meg, hogy milyen lehetőségeink vannak a fenti problémák megoldásának elősegítésére, a „híradás” szemszögéből. Nagyon fontos tény, hogy a felszámolás hatékonyságát döntően befolyásolja a jól szervezett és egymással interoperábilis infokommunikációs rendszerek működtetése, melynek az egyik sarkalatos pontja az alkalmazó állomány kiképzettsége, a különféle szervezetek „összekovácsoltsága”. Ez rögtön több problémát is felvet. Ismereteim szerint a különféle rendvédelmi szervek, a katasztrófavédelmi szervek felszámolása során együttműködésre kötelezett (ill. arra kötelezhető) szervek, szervezetek több évtizede ilyen jellegű gyakorlatot nem hajtottak végre, így összekovácsoltságról nem beszélhetünk. A másik sarkalatos pont, hogy van-e együttműködésre alkalmas kommunikációs rendszerünk. Jelenleg a még bevezetés alatt álló TETRA típusú rendszeren és a mobiltelefon-szolgáltatók rendszerein kívül nincs valódi közös együttműködési lehetőség a BM és HM végrehajtó szervei között. Az általunk használt híradó eszközök csak elvétve találhatók meg pld. a rendőrség eszközparkjában. Azt, hogy valaki tudja e kezelni, ill. vannak e rá kiadva pld. frekvenciák, vagy különféle, a rádióforgalmazást elősegítő és biztosító okmányok, csak találgatni tudom, de rossz sejtéseim vannak... A katasztrófavédelmi szervek is teljesen más eszközparkkal rendelkeznek, a mentőkkel, tűzoltókkal, vízügyesekkel, stb. való közvetlen kommunikáció részünkről csak illúzió. Sajnos le kell szűrni azt a következtetést, hogy együttműködési feladat során a jelenlegi eszközeink nem alkalmasak kommunikációra, „csak” a saját „belső” híradásunk megoldott.

Felmerül a kérdés, hogy akkor minek a jelenlegi stratégiai és (rég) tábori hálózat, egyáltalán alkalmas e bármilyen nem öncélú feladatra Magyarországon belül. Megítélésem szerint az állandó „béke-rendszerünk” alkalmas a katonai erők gyors mozgatására, szervezésére, irányítására a meglévő vezetékes, a mikrohullámú és az analóg rádiós eszközök segítségével is (akár az RH sávban is), de elsősorban a centralizált vezetési rendszer miatt, hiszen a katonai felsővezetés valós idejű információkkal rendelkezik, ill. rendelkezhet a kialakult helyzetről és az elképzelhető megoldásokról. A gond a különféle társszervek közötti közvetlen együttműködés során jelentkezik, amikor gyors helyi döntésekre van szükség, de a végrehajtó katonának minden esetben tájékoztatni kell az előjáró szerveket. Ráadásul egyáltalán nem biztos, hogy vezetékes összeköttetési lehetőség rendelkezésre fog állni. Az esetek döntő többségében a vezetékek nélküli kommunikációra kell támaszkodni, különösen „terepen”. A hatékony munka ebben az esetben a „kölcsonkapott” eszközökön valósítható csak meg. A másik problémája ennek a kérdésnek az, hogy a bázisállomások rendszerének megsérülése esetén a katasztrófa-súlytotta területen azok pótlása, ill. javítása körülményes lehet, ráadásul erős forgalmi torlódás alakulhat ki pld. a GSM struktúrákban, mely teljes „távközlési forgalmi dugót” eredményezhet. A TETRA típusú rendszer ez ellen csak annyiban védettebb, hogy a prioritási rend biztosíthatja a vezetők kommunikációját, ha nem esik ki túl sok bázisál-

lomás⁵¹ és beleférünk a hatótávolságba. Mindezek alapján én úgy látom, hogy egy nagyterjedésű katasztrófahelyzet esetén egységesen előnyben kellene részesíteni a helyi feladatokra a korszerű, FH és DSS üzemmódokat is ismerő URH rádiókat. Ezen eszközök – bár jelenleg sebességben korlátozással – adatátvitelre is alkalmasak, így valamennyi szervezet közötti infokommunikációra alkalmasak lehetnének és szükség esetén felfűzhetők a társszervek országos rendszereire is. A nagyobb távolságú összeköttetésekre szóba jöhet RH rádió is. Szerencsés esetben a meglévő analóg RH eszközeink korszerűbb, legalább FH üzemmódot is alkalmazó rádiókra való cseréje – hatékony és informatikával segített frekvenciamenedzsmenttel – a terjedési sajátosságokból adódó problémákat is megoldja, valamint így lehetőség lenne akár RH adatátvitelre is. Magyarországi viszonyok között nincs szükség nagyteljesítményű RH rádiókra (ez számításokkal is igazolható), ezáltal lehetőség nyílik a társszervezetek ilyen jellegű eszközökkel való ellátására is, hiszen nincsenek nagy méretek, nincs bonyolult kezelés. Ezen két eszközpark képes biztosítani az esetlegesen működő többi mellett az infokommunikációs csatornák további „duplikálását”, az „összeköttetés minden körülmények között” elv megvalósítását, a valódi együttműködés lehetőségével. Ráadásul a Magyar Honvédség mikrohullámú rendszere szükség esetén átveheti, pótolhatja, ill. kiegészítheti – bár több, pld. területi, ill. felhasználói korlátozással – a kieső országos távközlő hálózatok egy részének szerepét a katasztrófahelyzet idejére. Természetesen van még más lehetőség is, de sajnos korlátai vannak. Az egyik ilyen a műholdas eszközök alkalmazása, de az ára mellett a megfelelő számú eszköz beszerzése és elosztása is tetemes költséget jelentene. Nagy mennyiség beszerzése és utána a tárolása, várva a következő problémás helyzetet, igen drága és felesleges, mert a fenti eszközök ki tudják váltani. Tömeges alkalmazását nem tartom célszerűnek. A másik lehetőség a troposzféra rádiók újbóli alkalmazása lenne, mely akár radioaktív sugárzás esetén is képes rádiócsatornát biztosítani, a jelenlegi technikák esetén akár száznál is több távbeszélő csatornával, ill. az ennek megfelelő adatátvitellel. A gond csak az, hogy a hatótávolság kb. 350-400 km közötti, ezáltal az országon belüli alkalmazás lehetősége eléggé korlátozott. Lehetőségként szóba jöhetne pld. a WiMAX rendszerek alkalmazása is, de ez a technológia katonai szempontból jelenleg még nem kiforrott és igen sok nyitott biztonsági kérdést hordoz, de a jövőben mindenképpen számolni kell majd vele. Összességében a korszerű, szórt spektrumú üzemmódban dolgozni képes és adatátvitelre is alkalmas URH és legfeljebb közepes teljesítményű RH rádiók alkalmazását látom a minden feltételt kielégítő megoldásnak az országon belüli infokommunikációra, mely támaszkodik a stratégiai digitális mikrohullámú rendszerünkre és digitális kapcsolóközpontokra.

⁵¹ Lásd: 2001. 09. 11-i helyzet

Doktrínáink kimondják, hogy Magyarország érdekeit külföldön is kell érvényesíteni, a katonai- és politikai szövetségeseinkkel együttműködésben. Ebből az is következik, hogy meg kell vizsgálni azt, hogy a Magyarországon a katonai hírközlésben alkalmazott műszaki megoldások kivihetők, vagy sem a „missziós” feladatokra. Értékelni kell, hogy mely megoldások alkalmasak a hazaitól eltérő körülmények között és melyek nem. Kiindulásként megállapítható, hogy a magyar katonák az eddigiekben elsősorban műszaki, egészségügyi, őrzésvédelmi, konvojkísérési, szállítási feladatokat láttak el. Az adott feladat egyből jelzi, hogy egy szűkebb terület helyi híradását, vagy nagyobb távolságok – akár 100-150 km, vagy több – áthidalását, pld. menethíradást, bázisok közötti híradást, kapcsolattartás a hazai erőkkal, stb. kell biztosítani, alapvetően saját eszközeinkkel. Az igen sokféle szituáció más-más műszaki lehetőségeket igényel, melyeket a szerintem legfontosabbnak tartott szempontok szerint foglaltam táblázatba. Természetesen más szempontok is lehetségesek, pld. légierővel való együttműködés, haditengerészeti erőkkel való kapcsolattartás, stb. melyek tovább bonyolítják a műszaki-katonai helyzetet.

A különféle helyzetek alapján látható, hogy az eltérő típusok kombináltan jelentkeznek. Katonailag és műszakilag is belátható, hogy a megbízható összeköttetés érdekében a legrosszabb szituációra („worst case”) kell felkészülni, így a kevésbé problémás helyzetekben is működőképesek maradhatunk. Nagyon fontosnak tartom megjegyezni, hogy nem célszerű sokféle rendszert tartani „talonban”, hiszen jelentősen megdrágítaná és megnehezítené a készletezést, tárolást, karbantartást, utánpótlást, valamint a kiképzést. Mindenképpen célszerű ragaszkodni a minél kevesebb fajta műszaki megoldáshoz, de azok a leghatékonyabbak legyenek minden területen.

Külföldi misszió			
I. A feladat jellege szerint			
Helyi (pld. települések)	Távolsági		
	Mobil feladat (kis- és közepes távolságokra)	Nagy távolságú kapcsolattartás	
		Külföldi bázisok és együttműködők	Hazai erők felé
Többnemzetiségű környezet, interoperabilitási kérdések			

II. A földrajzi terület sajátosságai szerint		
Sík, vagy alacsony dombvidék vidék	Erősen tagolt hegyvidéki, magashegységi környezet	

III. Humán környezet szerint		
Baráti, ill. semleges környezet	Ellenséges környezet	
	Teljes ellenőrzés alatt áll	Csak részleges ellenőrzés valósítható meg

IV. Infrastrukturális környezet		
Infrastruktúra nélküli környezet	Gyengén ellátott, vagy rombolt környezet	Jó, működőképes infrastruktúra

Ez a költséghatékony rendszerüzemeltetés egyik fontos peremfeltétele. Ebből következően célszerűen olyan eszközök és megoldások kell hogy szóba kerüljenek, melyek a következő körülmények között is hosszú ideig biztosítják a hatékony csapatvezetést:

- Infrastruktúra nélküli, ellenséges, katonailag csak részben ellenőrizhető környezetre való felkészülés
- Kis, közepes és nagytávolságú összeköttetésekre egyaránt alkalmas rendszerelemek, melyeknél a terjedési sajátosságokból adódó problémák a rendszerelemek automatikus és gyors felcserélhetőségével igen gyorsan és hatékonyan megszüntethetők
- Törekvés a maximális interoperabilitásra

A fentiek alapján a tervezett hazai tábori rácsponi rendszert alkalmatlannak tartom ilyen jellegű külföldi feladatokra történő felhasználásra, hiszen igen sok feltételnek nem felel meg. Mindez mellett az elemek között vannak olyanok, melyek alkalmazhatók lennének. Az elemzési fő szempontok a következők:

- A kinti alakulatok nem önállóan, hanem elsősorban más tagországok kötelékében hajtanak végre feladatot, legfeljebb csak néhány rendszerelemet érdemes kivinni, területlefedő rácsponi hálózatot nem
- A rácsponi elemek mikrohullámú átjátszó funkcióra – ellenséges területen – a nehéz védhetőség és a nagy saját védőerő lekötés miatt nem hasz-

nálhatók, ráadásul erősen tagolt hegyvidéki területeken az optimális láthatóság és hatótávolság nem biztosítható (ez ideálisan is max. 50-70 km lehetne, bár a tervezett távolság eleve kisebb!)

- A mobil digitális kapcsolóközpontok valójában csak táborokban telepíthetők (ott viszont lehetőség van a különféle nemzeti rendszerek összekapcsolására a különféle interfészek alkalmazásával)
- A harcászati relék esetén ugyanolyan jellegű a felmerülő problémacsoport, mint a mikrohullámúnál, – csak a hatótávolság, frekvencia és kapacitás más: valamennyi alacsonyabb... –, ezért nem kívánom részletezni
- A rádiófelvevőpontok rendszere a táborok környékén, ill. a mobil erőekkel való együttműködésben jól használható, védett üzemmódok alkalmazása esetén (szórt spektrumú üzemmódok) hatékony, zavarmentes lehet. Probléma az erősen átszegdelt terepeken történő URH összeköttetéseknel adódhat, ahol jelentős hatótávolság-csökkenéssel is számolni kell. Menethíradás esetén a jelenlegi URH eszközeink 50-70 km-nél optimális terjedési viszonyok között sem képesek nagyobb távolságra „ellátni”, így más eszköztípust kell alkalmazni, pld. RH rádiókat. A felvevőpontok jól működtetett és szervezett, automatizált hálózat- és frekvenciamenedzsment segítségével gyors átkapcsolásokat tehetnek lehetővé a különféle rádiórendszerek között, valamint képesek biztosítani a rádiócsatornák továbbítását – a kapcsolóközpontokkal való együttes üzemeltetés esetén – más nemzeti rendszerei felé, ezáltal a jelenleg meglévő digitális inkompatibilitások hatása jelentősen csökkenthető.
- A nagytávolságú és menethíradások távolsági összeköttetéseire jelenleg műszakilag csak a műholdas és az RH összeköttetések alkalmasak, párhuzamos üzemeltetésük a rendszer megbízhatóság érdekében indokolt, egymást kölcsönösen kiegészíthetik. Az ilyen jellegű felhasználás során nem szükséges sok műholdas eszköz egyidejű üzemeltetése, ezáltal a bekerülési/beruházási költség ésszerű keretek között tartható.
- A troposzféra rádiók alkalmazása a korábban tárgyalt távolságokra indokolt lehet, mert képes kiváltani műholdas csatornákat szélessávú adatátvitel mellett, ráadásul a földi nagytávolságú mikrohullámú átjátszást is meg lehet velük oldani. Lehetőséget teremthet pld. akár Irakból átjátszásokkal a NATO műholdas rendszer által lefedett területek elérésére is. Az más kérdés, hogy biztosítani kell a különféle tagországok troposcatter eszközeinek kompatibilitását, vagy jobb esetben interoperabilitását, hiszen több eszköz láncolt átjátszásáról van szó, melyet a Magyar Honvédség jelenleg és valószínűleg a későbbiekben sem fog tudni önállóan felvállalni.
- A vezetékes eszközökkel nem kívánok foglalkozni, hiszen azok csak a táborokban, ill. a meglévő civil infrastruktúra felhasználásakor kerülhetnek szóba, igen sérülékeny rendszert alkotnak, ráadásul telepítésük is hosszadalmas, védelmük sem régen, sem jelenleg nem megoldott, a kor-

szerű hadviselésből adódó dinamikus feladat-végrehajtást csak gátolják. Megítélésem szerint elsősorban hazai viszonyok esetén, ill. baráti (esetleg semleges) külföldi területeken lehet csak jelentősége, bár könnyű célpontja lehet bármilyen szabotázsaknak.

A műszaki berendezések működtetéséhez elengedhetetlen nagyhatásfokú, kisméretű, könnyű áramforrások, aggregátorok rendszerezítése, párosulva lehetőleg energiatakarékos berendezések alkalmazásával, a minél hosszabb önálló üzemeltethetőség elérése érdekében. Célszerű előnyben részesíteni olyan sugárzó eszközöket, melyek képesek adaptív teljesítményszabályzásra is. Sajnos tudomásul kell venni azt is, hogy a különféle digitális kapcsolóelemek, multiplexerek, számítógépes eszközök igen sok hőt termelnek, klimatizálásuk – *különösen sivatagi, ill. trópusi, de néhány területen a mérsékelt égövi (nyári időszak) területeken is* – elengedhetetlen, és más hiedelmekkel ellentétben nem a katonák hűsölését szolgálják. Ez sajnos az energiafelhasználás jelentős megnövekedését okozza, tehát a felhasználandó eszközök száma ugrásszerű teljesítményfelvétel-növekedést okoz. Egy korszerű tábori harcvezetési ponton ma már nem elegendő az, hogy a gépjárművezetőkben áramforráscsoport kezelő ügyeleti szolgálatot szervezünk. Külföldi tapasztalatom szerint képzett energetikai szakemberre van szükség, korszerű, az energiaellátást hatékonyan biztosító automatizált áramellátó, átkapcsoló, stb. funkciókat ellátó mobil „trafóházakkal”. Az más kérdés, hogy kis létszámú erők esetén a külföldi feladatoknál nem indokolt teljes vezetési pontok kitelepítése és alkalmazása, de hazai feladat-végrehajtás során – *különösen, ha az országos áramellátás is megsérült* – nem szabad elfelejtenünk erről az „apróságról”.

Mindezen megfontolások figyelembevételével külföldön tömegesen a kis és közepes teljesítményű URH, a kis, közepes és kiegészítő modulálással szükség esetén nagyteljesítményűvé módosítható RH rádiók alkalmazását tartom elengedhetetlennek, adaptív teljesítményszabályzással és szórt spektrumú modulációs eljárások alkalmazásával, beszéd és adatátvitelre egyaránt. Rendszerbe történő integrálásuk hatékony automatizált hálózat- és frekvenciamenedzsmenttel működtetett rádiófelvevőpontok és digitális kapcsolóközpontok együttes alkalmazásával érhető el, mely biztosítja az átjárást akár más nemzetek rendszerei felé is. Kiegészítő megoldásként a kis eszközszámmal műholdas, valamint a néhány (nagy távolságú) szegmensét kiváltó troposzféra rádióállomások alkalmazását látom célszerűnek. A berendezések kiválasztásánál döntő szempontnak kell lennie a hosszú önálló üzemidőnek – természetesen ez nem mehet pld. a hordozhatóság rovására. Amennyiben az eszközpark kiválasztása során a felhasználó-barát eszközöket előnyben tudjuk részesíteni, az nagy mértékben elősegítheti az anyaországbeli adaptációját is és az országon belüli feladatokba történő beintegrálását. Ebben az esetben mindenképpen célszerűvé

válí a rendvédelmi, katasztrófavédelmi szervek, szervezetek típuseszközökkel való ellátása is, a hatékony együttműködésünk érdekében. Sajnos tisztában vagyok vele, hogy ez sok esetben szervezeti (önállósági) érdekeket sért, ennek ellenére az a véleményem, hogy csak az egységes hazai – és természetesen külföldön is használható – eszközpark lenne képes feloldani a kommunikáció terén jelentkező technikai anomáliákat, inkompatibilitásokat. A jelenleg teljesen működő hazai rendszerek esetén – a TCP/IP alapú informatikán és esetleg a GSM rendszereken kívül – nem látok interoperábilis magyar katonai/rend- és katasztrófavédelmi megoldásokat, miközben a katonák között jól ismert, hogy ez az egyik legkívánatosabb cél a NATO hosszú távú terveiben is. Sajnos jelenleg én inkább csak a párhuzamos megoldások rendszerét érzékelem, ami a jövőben egyre-inkább tarthatatlanná fog válni.

Rövid elemzésemmel rá kívántam mutatni egy általam a legcélszerűbbnek tartott útra és néhány műszaki-katonai megfontolásra annak érdekében, hogy a honvédség és más szervek, szervezetek infokommunikációs rendszereit hatékonyan lehessen együttműködtetni az emberi életek megmentése érdekében katasztrófahelyzetek felszámolása során. Nem elhanyagolható szempont az sem, hogy irányt kellene váltani egy minél homogénebb országos rendszer megvalósítása érdekében, melynek gazdaságossági szempontjai is jelentősek lehetnek. Az, hogy végeredményben a külföldi feladat-végrehajtás szemszögéből csatoltam vissza, szerintem egyáltalán nem hiba, hiszen ami odakint (harc-helyzetben) kipróbált és hatékony, az idehaza katasztrófa helyzetben is működőképes maradhat. Természetesen nem kívánok semmilyen gyártóra, ill. annak eszközére javaslatot tenni, hiszen az nem az én kompetenciám. A leírtak viszont elősegíthetik néhány szemponttal akár egy tender műszaki-katonai elvárásainak, követelményrendszerének megfogalmazását is.

Irodalomjegyzék:

1. http://www.kulugyminiszterium.hu/kum/hu/bal/Kulpolitikank/Biztonsagpolitika/Nemzeti_biztonsagi_strategia.htm
2. http://www.cab.u-szeged.hu/local/ssadm/2003_levelezo/gyp/Tetra.htm
3. <http://www.shoshin.uwaterloo.ca/~jscouria/GSM/gsmreport.html>
4. <http://www.ham.hu/radiosatvitel/savkiosztas/>
5. http://en.wikipedia.org/wiki/High_frequency
6. http://en.wikipedia.org/wiki/Very_high_frequency
7. <http://www.tmcnet.com/channels/wimax/what-is-wimax.aspx>

Erik PÁNDI:

Closed-purpose systems contra governmental centre
of electronic public services

1. Professional-political background

Apparently, during the last more than one and a half decade, there had been very significant, complex and sophisticated changes in Hungary. The complete reorganization of the **economic and legal circumstances**, the improvement in the field of **communication technology**, furthermore the changes – *according to the sample to be applied in the western societies with more developed economy* – in **governmental technology** and ideology supported by the former were launched simultaneously, affecting in this way completely the operation and maintenance of the communication systems serving the government and other administrative organisations. The modification of the **economic structure** of Hungary has gradually terminated the dominance of state property, the market economy taking shape has assisted the spread of a modern communication and information technology in Hungary. With the development of technical assets and systems the assortment of communication services became wider, however, the „three-legged”, liberalised, **competition-based** market (servicing sphere with many participants, individually functioning authority, and controlling governmental organisation) was only formed at the beginning of the 21st century.

The **closed-purpose (telecommunication) systems** as legal category were introduced by the Act LXXII of 1992⁵² paragraph 2, article (3), which was also confirmed by the Act on Electronic Communications C of 2003⁵³ paragraph 1, article (2): „(2) *This Act shall apply in respect of electronic communications networks, being distinct due to their purpose (private networks), used exclusively for meeting special government, national security, judicial, law enforcement, and national defence requirements, subject to the exceptions contained in the relevant acts and specific other legislation.*” [1]. The Act on Telecommunication authorized the Government to specify the rules of the operation of closed-purpose systems, which was completed through the **governmental decree No 50/1998 (III.27.)** on closed-purpose telecommunication networks, that has been modified several times. Basically, the above regulations made and make possible that the communication systems, which have been improved and developed since the middle of the last

⁵² abbreviation: Tt. The referred act was superseded by the Act No XL of 2001 on telecommunication, paragraph 103, article (8) point e) on 23 December 2001

⁵³ abbreviation: Eht. (Act C of 2003 on Electronic Communications) the Act on telecommunication was superseded by Eht. paragraph 165 article (1) point a) on 1 January 2004

century still exist. The structure of participants maintaining the systems and the connections between them have definitely changed with the modification of **legal circumstances**. A significant part of Hungary's communication infrastructure became private property through the acts and other legal regulations related to the economic and telecommunication sectors, as the approach has also changed, which did not allow earlier the changing of the dominant role of state property due to military and interior safety interests [2].

At the beginning of the '90s, the extensive changes and the spread of communication (multimedia) services even in Hungary inspired the government to assist legally the installation of new possibilities into the work process for the establishment of the **servicing** authority modell, and for the long-run setting up of the **electronic government**. The necessity of the alteration of government technics and the serving communication system has actually came to the front in parallel with Hungary's joining the continental association systems, when the co-ordination of courses and the responsibility for the controlling of individual executive units were moved from the ministries to the Prime Minister's Office (PMO).

Since 1999, complete changing of the approach can be observed, that was affected mainly by former failure, convergence of technology and communication systems, furthermore the continuous strengthening of expectations concerning the serving state and the electronic government. In the further developmet conceptions the material and organisational principles declared by telecommunications politics⁵⁴ have definitely appeared, according to which governmental telecommunication is operated applying the existing resources of governmental and state majority owned managing organisations, through the competition of servicing units and simultaneously these are supervised by governmental organisations. On the other hand the question of – *firstly* – system set up for establishing the government providing services (Electronic Governmental Main Line Network) and the question of setting up the centralised radio-communication system (EDR: Egységes Digitális Rádiótávközlő Rendszer – Integrated Digital Radio System) had been entirely separated.

At the beginning of the century the EKG (EKG: Elektronikus Kormányzati Gerinchálózat – Electronic Governmental Main Line Network) was set up centrally and has become a dominant section of governmental communication by 2004. Its main services first of all assist the realization of data exchange, however, with the elimination of borders between the various specialities the preparation of the system for talking-purpose communication services. The realization of the EDR in the above organisational construction started by the end of 2005.

⁵⁴ governmental decision No 1071/1998 (V.22.) on telecommunication policy

In 2006, based on the related law – *in essence* – six closed-purpose system hosts⁵⁵ are appraised, who supervise on the whole more than thirty individual, nationwide communication systems, from which the systems of the military and home defence sectors can be considered dominant and determinative.

2. Recent changes in the legal measures

As for the home affairs organisations and the communication networks serving them the **Act No LV of 2006** on the listing of the ministries of the Hungarian Republic, furthermore the contents of the **Act No. LVII of 2006** on state administration organisations, and on the legal status of the members of the Cabinet and that of the under-secretaries resulted in remarkable changes. The tasks of the former Ministry of the Interior have been shared among the PMO, the Ministry of Justice and Law Enforcement and the Ministry of Local Government and Regional Development.

As for the communication networks serving the home affairs sector the situation is more complex, because the **governmental decree No 144/2006 (VI.29.)** paragraph 1, article (2) on instant changes required in the governance of executive information technology tasks declares – *among others* – that the supervision of the Telecommunications Service operating and maintaining so far the national main line network, furthermore the BM EDR VPN⁵⁶ centre and the supervision of the Central Data Processing, Election and Registration Office handling the various state data bases shall be included among the tasks and within the competency of the Minister governing the PMO. These two former home affairs organisations are directly governed by the cabinet officer of the PMO according to the **governmental decree No 1066/2006 (VI.29.) point 2 i)** on the assignment of the cabinet office in charge for administrative information technology.

In addition to the above, based on the contents of point c) of the **governmental decree No 1054/2006 (V.26.)** on the preparation tasks of reforming public administration, furthermore in Annex 1 of the **governmental decision No 2118/2006 (VI.30.)** the organisational changes and measures supporting the effective operation of state budget the Centre of Electronic Public Services under the supervision of the PMO shall be set up by 1 January 2007, which will include – *based on yet unidentified organisational concept* – the further public administration organisations: a) **Telecommunications Service**, b) **Central Data Processing, Registration and Election Office**, c) **Governmental Frequency Management Office**, d) **National Information Infrastructure Development Institution**. The Centre of Electronic Public

⁵⁵ the Minister of the Interior, the Minister of Defence, the Minister of Finance, the Minister of Justice and Law Enforcement, the Chief Prosecutor and the Minister heading the PMO

⁵⁶ BM EDR VPN: the centre controlling, supervising the application of (VPN) EDR services within the sector of the entire home affairs field, as a virtual network

Services will be probably controlled by the Electronic Governmental Centre, as a central organisation of the PMO.

3. Emerging troubles

According to the legal authorisation the individual organisations of the former interior affairs sector could possess closed-purpose network, that have been gradually set up since 1990. Consequently the Police Force, the Border-guards, the Disaster Protection force, the Central Data Processing, Resgistration and Election Office and the Immigration and Nationality Office have possess considerable telecommunication network. The Telecommunication Service provides main network services for the communication systems of the above, through its nationwide base infrastructure. The complex communication system set up in this way was known as the Integrated Digital Home Affairs Network, discharging it from compulsorily joining the EKG⁵⁷ [3].

3.1. Main problem

During the future relaization of the EU concpetion⁵⁸ of the state and the government the community decision-makers intend to reach, that the member-states in this field applied the directives compulsorily, which would mean that the quality of the Hungarian governmental execution shall be improved compulsorily. The organisational background⁵⁹ installed at the PMO is given, however, due to the division of the closed-purpose systems in the half-decade past the Electronic Government-centre could not reach the optimalization of the capacity of the EKG. Due to the above reasons the administrative “*incorporation*” of one of the largest main line service providers⁶⁰ is obvious and justified, but at the same time it will **discharge** both the Ministry of Justice and Law Enforcement and the Ministry of Local Government and Regional Development from having elementary impact on the operational process of the organisation serving the former Home affairs institutions with basic communication services, first of all when the safety of the services is not guaranteed by normative means or written agreement.⁶¹

⁵⁷ the listed exceptions are also specified in point 5.1.1 of the EKG Network Application Rules issued together with the governmental decree No 5/2004 (I.9.), in addition to which point 5.1.2 names a further organisation too

⁵⁸ e.g.: i2010 action plan

⁵⁹ which also supplies the duty of the EDR network host

⁶⁰ Telecommunications Service

⁶¹ due to negligence

3.2. Further troubles

The **difference in apprehension** between the proper professional organisations of the PMO and the operational practice of the telecommunication organisations of the former Ministry of Interior, that still exists can be considered a significant trouble. The core of this problem is that the PMO does not want to get into direct connection with the end-user, this point is solved indirectly, which is unrealizable among the units serving organisations also executing operative tasks. Beyond ensuring operational quality, this is also a question of safety.

We shall mention therefore, that the inclusion of private capital into the various development processes of the – *of safety character* – communication networks, furthermore the transferring of maintenance and operation related tasks to non-governmental organisations **cannot be always considered just economically**, several times a – *fiscally* – more adverse budget is taking shape.

Nowadays it is an emerging trouble, that the functionality of state administration is managed not by financing tasks, but through the financing of organisations, therefore recently the application of the “*mowing-machine theory*” privation practice has become general; in this way the former professional home affairs organisation have to manage their tasks – *many times full of professional-political expectations from the Union* – at Western-European maintenance costs and continuously decreasing financial facilities.

From the point of view of the former home affairs organisation the concentration of tasks in the PMO could mean, that the managing of debt accumulated due to intended under-planning taking into consideration – *only and exclusively* – financial reasons is to assist the cheap market positioning of monopolist telecommunication service providers⁶², terminating in this way the possibilities of direct enforcing of interests and maintenance at “first-cost”.

4. Summary

All in all we can say, that the PMO is presently in the possession of all the legal possibilities and authorization, which would assist the actual implementation of electronic public services. **The liability is however enormous**⁶³, as the rapid conversion of such operating structures is the purpose, the operational features and thorough knowledge of which are presently absent.

* * *

⁶² Magyar Telekom group and its interests

⁶³ and cannot be repeated according to the present practice

References:

- [1] <http://www.nhh.hu/dokumentum.php?id=menu&mid=625>
- [2] Török, Gábor (PhD): Az új hírközlési törvény néhány polgárjogi problémája, Az információs társadalom és a jog átalakulása – Magyarország az ezredfordulón, Stratégiai kutatások a Magyar Tudományos Akadémián, Workshop studies, Hungarian Academy of Sciences, Budapest, ISBN 963 508 377 7, page 210, 2002.
- [3] Governmental devree No 5/2004 (I.9.) on the modification of the Governmental decree No 50/1998 (III.27.) On the closed-purpose telecommunication networks, Magyar Közlöny, No. 2004/3., Budapest, page 153-154, 2004.

Bibliography:

- [1] ITTK Csoport: E-közigazgatás-Éves jelentés 2005., Budapest, 2005. December-2006. February
- [2] e-Government in the member states of the European Union, <http://www.egov-goodpractice.org/download.php?fileid=223>
- [3] i2010: az új stratégia – <http://www.itk.hu/infini2005/0609>

Erik PÁNDI:

Competitive civil service – queries of development

1. The conception of setting up the Centre of Electronic Public Services

Based on **point c) of the governmental decision No 1054/2006 (V.26.)** on reforming the public services, a proposal had to be made for the Government until 31 August 2006 concerning the setting up of the **Centre of Electronic Public Services** (EKK: Elektronikus Közzolgáltatások Központja). According to the Annex No. 1 of the governmental decision No 2118/2006 (VI.30.) on organisation changes and measures assisting the effective work of the national budget, the EKK shall be established as an individual budgetary organisation until **1 January 2007**, and at the same time the organisation of the information technology tasks of the various ministries into the new budgetary unit shall be also managed.

For the preparation of the establishment of the EKK, the **governmental decision No 1066/2006 (VI.29.)** a governmental expert was assigned for the period until 31 December 2006, who shall control civil information technology – *as a distinguished task in addition to controlling administrative information technology*. With the participation of experts the governmental controller has prepared the conception of setting up the EKK. Upon the establishment of the new organisation, the conception considers sparing in the operation, the demand for more effective and rational work and the strengthening of the serving and client focused features as the main purpose and basic requirement. The establishment of the new organisation together with the setting up of the organisational-institutional system ensuring the execution of the aims will confine simultaneous costs, abolish bureaucracy, simplify legal regulation and assist the shaping of new forms of e-democracy.

According to the conception upon the establishment of the EKK – *besides the strengthening and functional expansion of the Central Electronic Service System*⁶⁴ – central operation resulting economisation will be achieved through the concentration of the information technology operating organisations of the Prime Minister's Office (PMO) and that of the ministries.

The integrated courses, procedure orders and applications – *resulting from the integration of standards, regulation and quality policy* – ensure the public work-style operation based on more effective and rational administrative action. These services are supported by integrated information technology security solutions ensuring the protection of private data and undisturbed progress.

⁶⁴ based on the Act No CXL of 2004 (Ket.) its already functioning members are: the Electronic Governmental Main Line Network, the Governmental Portal, the so called "Client Gate", and the Governmental Client Information Centre

Through the consolidation of the presently redundant information technology and telecommunication systems (Integrated Central Main Line Network – EKG: Elektronikus Kormányzati Gerinchálózat), interior affairs and documentary networks, individual branch networks) the parallel operational costs will be eliminated. The consolidation of systems ensures the establishment of technical conditions of the connection between the systems of various purposes (EKG, EDR, Public network, NIIF) furthermore of the IP-based data- and voice integration resulting significant savings.

For the further development of services to be provided between the civil service organisations and the citizens and enterprises, furthermore for improving the level of these services, the central co-ordination ensures the effectiveness of controlling. In the framework of central co-ordination the EKK – *on the Electronic Government Centre of the Ministry of the Interior, integrating the Central Data Processing and Registry Office, the Telecommunications Service, the Governmental Frequency Office* – the e-government is responsible, as a central organisation it fulfils the function of the information technology centre. This organisation is electronically connected with the branch public service centres: a) Information Technology Centre of the Ministry of Finance, as the financial service centre,⁶⁵ the electronic service centre related to employment policy, labour policy and pension,⁶⁶ furthermore the electronic service centre related to healthcare and social insurance.⁶⁷

After the setting up of the new organisation single tasks and competence will be shaped through the merging and rational distribution of tasks presently proportioned and arising parallel:

- a) information strategy of the civil service, the elaboration of the related policy, the regulation and inter-ministerial co-ordination remain within the competence of the minister leading the PMO;
- b) the EKK as a central office will supply 1st degree authority duties, the controlling and supervision of electronic civil service (civil service information technology), it will be also in charge of central development and co-ordinate sectional development, furthermore control and supervise the operation of systems, networks, applications and databases; and the function of economic organisations operating the information technology security centre.

The resources required for the operation of the new organisation can be ensured from central budgetary estimates (for launching central investments

⁶⁵ with the networks of APEH (Tax Authority), VPOP (Hungarian Customs and Finance Guard), MÁK (Hungarian State Treasury)

⁶⁶ with the EMMA (Uniform Hungarian Labour Database) and the ONYF (Central Administration of National Pension Insurance Systems)

⁶⁷ with the systems of OEP (National Health Insurance) and TB (Social Insurance)

and developments), through the merging of branch information technology and telecommunication resources (for financing central operation), from the Operative Programs, and from the income of individual services (e.g. e-public procurement fee). Further⁶⁸ reform-related tasks:

- a) setting up the Uniform Central Client Service Centres;
- b) consolidation of the branch information technology systems and co-ordination with the central databases;
- c) analysing the facilities of *outsourcing* the information technology and telecommunication related tasks;
- d) taking over the databases (basic registries) by central operation;
- e) launching pan-European services specified by the EU.

2. Launching electronic services at the municipalities

As for the Hungarian municipalities the absence and arrears are determinant many times. Despite the governmental efforts the Internet developing procedures of the Hungarian municipalities still show „island-type” operation. It is the result of the inadequate information technology integration between municipal competence and duties, and of the absence of information technology education and standardization.

During the years past municipal information technology developments had been financed through GVOP-tenders (Economic Competitiveness Operative Program), however, the problem with this form is, that the application can only aim development and investment both on Union and Hungarian level, the operation of the systems cannot be included. Therefore municipal investments include risks, as for the projects worth 300-400 million HUF the same sum should be added within a few years. It means, that the computer systems to be installed into the regional territories will be unworthy in three years, provided that the certain municipalities do not spend on HW and SW development.

The online availability of civil services in case of the municipalities is poor, as practically only the possibility of registering the changes in the postal address is wide-spread in practice. At the same time this service is only operated by tenth⁶⁹ of the municipalities possessing a web-page, on a certain level and in case of most of them just information is available on this service.

The transaction of authority certificates, permissions and the operation of public libraries were materialised at the same rate. Most of the services, however, did not reach this level, provided that the municipalities have tried to launch electronic services in these fields. The operation of the integrated digital back-office service is required firstly in bilateral interaction. Only 2 % of the municipalities operate such service connected to the individual services,

⁶⁸ 2007-2009

⁶⁹ 13 %

while 90 % of them does not. The remaining 6-8 % plans only to install the service. Based on earlier analysis figures⁷⁰ for most of the municipalities the main problem is still the acquisition and the maintenance of the basic infrastructure, that are highly demanded. The second significant problem is the absence of internet connection, or the deficiency of the existing connection. Only 8 % of the municipalities possess written information technology and 3 % information society strategy.

3. Summary

The definite purpose of the PMO is to set up in Hungary a uniform communication and service structure through the EKK to be formed from central organisational processes. This structure would require only single entrance. It can be definitely specified among the purposes, that even citizens living in smaller places, who are not familiar with electronic administration or with the application of internet could enjoy the benefits of remote transaction of affairs, additionally the participants⁷¹ of municipal administration could manage more difficult cases instead of clients.

The reform of public service, that is making its operation more rational, faster and more transparent is the essential and acute condition of the establishment of the competitive Hungarian public service⁷². It is an important question, how the decision makers can take advantage of the creative destruction being started nowadays, how much the benefits of the information-technology assets are emphasized in the alteration of service-side courses.

As for the future, the artificially separated electronisation process of central and municipal administration, that is parallel in many cases shall be also co-ordinated. The non-coordinated development policy is especially true for the developments executed with the distribution of EU resources, furthermore in case of the parallel improvement of wide systems without co-ordination.

Bibliography:

[1] ITTK Csoport: E-közigazgatás – Éves jelentés 2005., Budapest, 2005. December-2006. February

[2] e-Government in the new member states: mission impossible?
[http://www.politech-](http://www.politech-institute.org/review/articles/ZALISOVA_Irina_volume_1.pdf)
[institute.org/review/articles/ZALISOVA_Irina_volume_1.pdf](http://www.politech-institute.org/review/articles/ZALISOVA_Irina_volume_1.pdf)

[3] T-Systems: Az Elektronikus Kormányzati Gerinchálózat (EKG) kínálta lehetőségek, „Communication 2005” International professional academic conference, Zrínyi Miklós National Defence University, Budapest, page 575-582, ISBN 963 7060 11 1, 27th October 2005

⁷⁰ GKleNet

⁷¹ recorders, administrators

⁷² state- and municipal administration

1. Introduction

Ever since the invention of radars getting protection against them has become an on-topic need, that is, the problem of low radar cross section. During the years several methods have been developed based on different concepts [2]. With the fast improvement of signal processing capabilities these methods have become more and more sophisticated. Simultaneously, detection techniques have also improved in radar technology.

The novel LRCS method, developed by us, is a contribution to the already existing LRCS techniques. Unfortunately there is no general solution for the problem of LRCS, henceforth, the method introduced is not it either. However, according to our results our LRCS method, based on CRCS, causes significant RCS reduction, this effect cannot be compensated by the radar.

According to our researches the possible utilization fields of LRCS are not confined to the field of radar technology, it is also applicable on the field of communications, for example to reduce fading situations or to create diffuse measurement environment in measurement technology.

2. Low CRCS Theory

The definition of RCS: the power arriving in unit solid angle at the object divided by the power radiated by the object in unit solid angle. In other words: it defines the scattering-strength of the object for a given orientation.

When an object is radiated by EM waves, arriving from a narrow solid angle range, it will distribute the incident power in the space in a larger solid angle range. The exact distribution of the reflected power in the whole solid angle range is influenced by the shape and the electric properties of the object, more precisely the reflection of the surface elements of the object. The smaller the wavelength compared to the dimensions of the object is the more of such surface elements take part in creating the scattered field and the more complex the RCS characteristics will be.

This concludes that if all points of the surface of the object have passive reflection, then, for example in a monostatic case, the backscattered power density is usually smaller than the radiating one. Forming the shape of the object does not influence the backscattered total power of the object certainly, only the reflected power density towards a direction can be influenced supposing power density incidence onto the object from a certain direction.

It is also obvious that design for a general bistatic arrangement is not possible, therefore, monostatic arrangement is usually supposed, when design-

ing the shape of objects. Typically the aim is to achieve the least possible backscattered power.

The total backscattered power can be reduced by the utilization of absorber materials. It is also possible to be achieved electronically, for that the ability to control the reflection of the surface elements of the object is necessary, a way to achieve that is placing antenna elements on the surface of the object [2].

The idea to match the antennas perfectly (ending them with the wave impedance of the antennas) might arise, however, the problem with this solution is that the antennas have structural reflection as well, which is caused by the improper matching between the antenna waveguide and the free space. Modification of the previous solution is possible by achieving such an ending at the antenna outputs that compensate the reflection of the structural reflection. The problem with this is that the structural reflection is not constant, it varies with the direction of incidence of the radiating EM waves. A good solution would be to measure the direction of arrival of the EM waves and to synthesize reflection with the help of the known direction dependent RCS characteristics of the object that extinguishes the structural reflection in the given direction. Nevertheless, this is not soluble effectively in the case of short and agile impulses.

If the reflected signal could be placed outside of the receiver filter band, for example by imitating Doppler-shift, then this could be deceptive information. However, with this maneuver nothing else was done but the displacement of the signal to another filter block of the MTD filter system.

A better method is to attempt to spread the frequency spectrum of the incident signal by only controlling the reflection of the surface elements of the object. If the reflection is passive (its absolute value is less than unit) the power that is inputted into each filter is less, and if the bandwidth of the receiver filter is narrower than the bandwidth of the modulation then some of the power of the reflected power will „vanish”, hence we reduced virtually the RCS.

3. Low CRCS Simulation

In the followings few simulations are shown, based on the previous idea. In the simulations the radiation patterns of the elementary radiators are disregarded, that is we supposed isotropic radiators. Each antenna element is modulated independently by evenly distributed white noise, via I-Q control signals. In the case of unit distributed noise the amplitude can be achieved to remain in the $[0, 1]$ interval. A stricter requirement is to achieve the independence of the radiation patterns that follow each other in the simulations. If the bandwidth of the modulating noise is significantly broader than that of the receiver filter, then the desired independence is ensured. In other words: the receiver will sense an average radiation pattern, which can be considered the

more isotropic the broader the bandwidth of the signal compared to that of the receiver is. The isotropic character is helped by the fact that radars typically use multiple impulse packets instead of just a single impulse for decision-making, the impulse number of such packets usually being between 20 and 60. Since, these impulses follow each other with large time gaps, independence between them, subsequently the isotropic character is ensured automatically.

Figure 1. shows the arrangement used in the simulations. The arrangement is a linear equidistant antenna row, where the perpendicular direction towards the row is considered zero degree. Degrees are measured in θ .

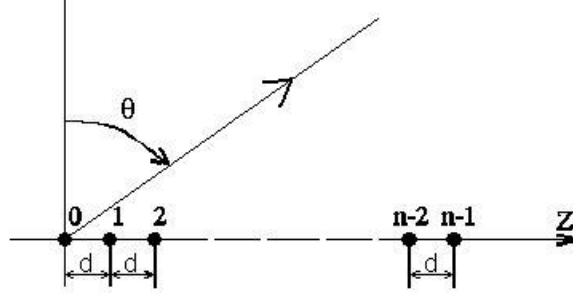


Figure 1.: 1D antenna elements arrangement

Generally, the directional factor of antenna systems can be calculated by the excitation-weighted sum of the electric field strengths created by the antenna elements in a certain direction. Therefore, if $F(\theta)$ is the directional factor, then it can be calculated by (1).

$$F(\theta) = \sum_{k=1}^M h_k e^{-j\beta k d \sin(\theta)} \quad (1)$$

During the simulations the excitation was determined by 2 variates, as seen in (2).

$$h_i = \xi_i e^{-j\nu_i} \quad (2)$$

To every directional factor different realizations of these variates belong. The vector variate $\underline{\xi}$ contains the amplitudes of the excitations of antenna elements, while $\underline{\nu}$ contains the phases of it. Since the control process is done in I-Q and the maximal amplitude value is unit the variates are limited to the range in (3).

$$\xi_i \in [0,1], \nu_i \in [0,2\pi] \quad (3)$$

Figure 2. shows the simulation results obtained according to principles above for a 32 element antenna row. The green curves show the directional

factors for different realizations of ξ and $\underline{v}$, while the blue curve shows their average.

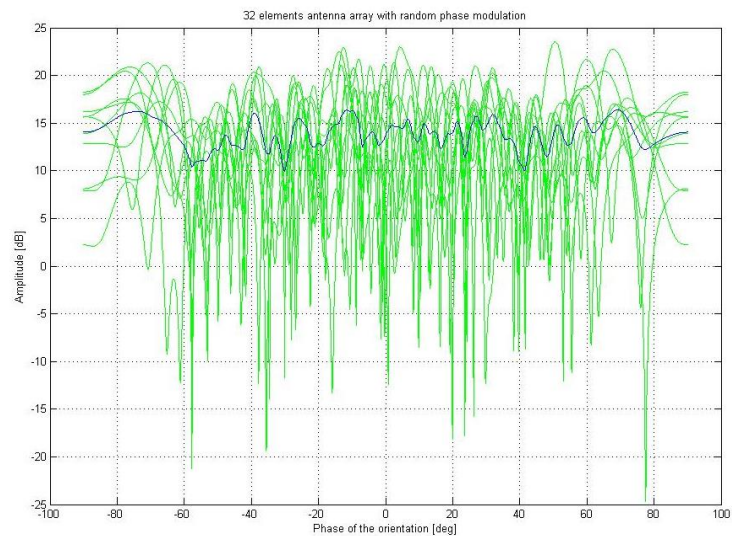


Figure 2.: The directional factors of the 1D antenna system (10 realizations) and their average.

The horizontal axis shows θ in degrees, while the vertical axis shows the absolute value of the far field strength in decibels.

Figure 3. shows 100 realizations for the same antenna structure and their average. As expected, the variance of the averaged directional factor decreases with the growth of the number of averaged directional factors.

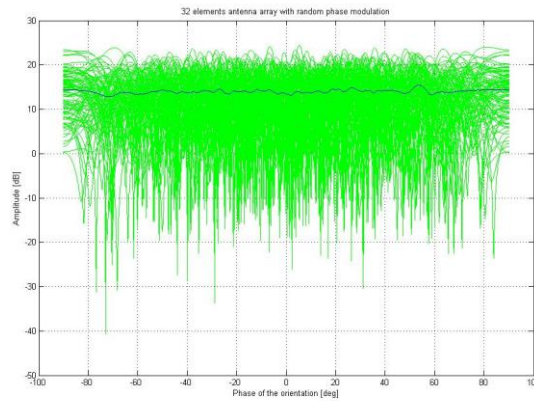


Figure 3.: The directional factors of the 1D antenna system (100 realizations) and their average

As the result we obtained an antenna system that behaves like an isotropic antenna even in a short period of time, that is, in average it radiates the same power in all directions. From the aspect of the theory it does not represent a novel approach to control the reflections of the antenna elements, supposing bistatic arrangement, all other conditions of the simulations remaining the same as before. Additionally, the antenna arrangement is 2D in this case, a 8x8 antenna grid. Figures 4., 5. and 6. show the same on the right side: a reference to compare the RCS decrease to. The figures on the left side show the average of the directional factor created by noise modulation. Figure 4. shows the measured noise modulated directional factor, without averaging. In figure 5. the averaging number of the directional factors is 10, in figure 6. 100.

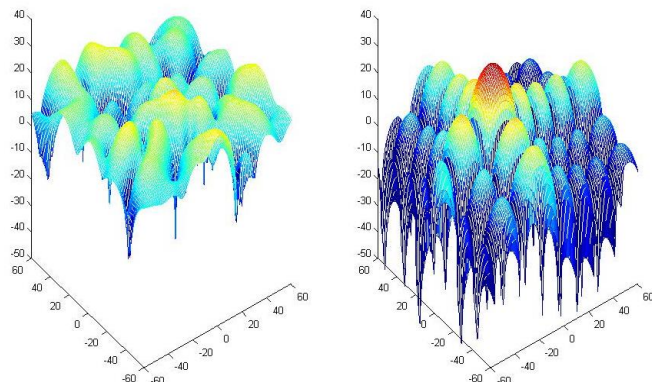


Figure 4.: The RCS of the 2D antenna system (1 realization) on the left and the RCS of the same antenna system in the case of deterministic control ($\theta=10^\circ$ and $\varphi=20^\circ$) on the right.

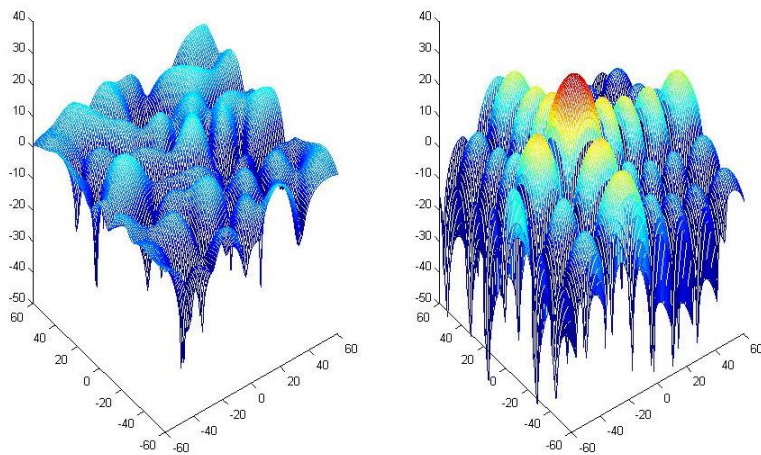


Figure 5.: The RCS of the 2D antenna system (10 realization) on the left and the RCS of the same antenna system in the case of deterministic control ($\theta=10^\circ$ and $\varphi=20^\circ$) on the right.

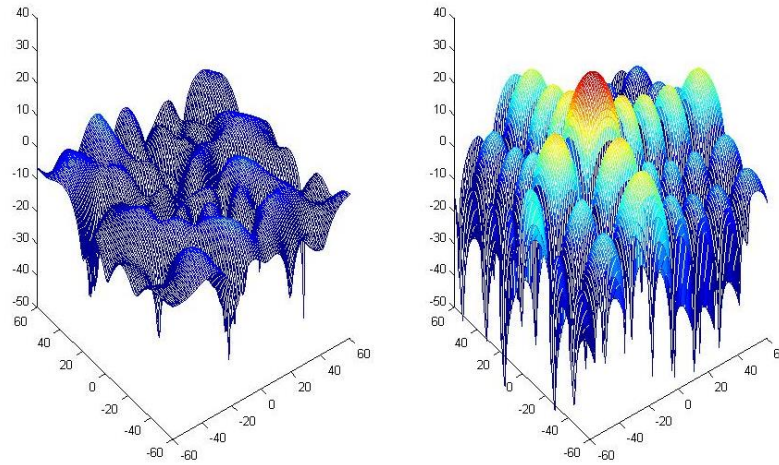


Figure 6.: The RCS of the 2D antenna system (100 realization) on the left and the RCS of the same antenna system in the case of deterministic control ($\theta=10^\circ$ and $\varphi=20^\circ$) on the right.

In figures 4., 5. and 6. the azimuth and elevation angles are shown on the horizontal axes in degrees, while the vertical axis shows the monostatic RCS in decibels. As in the 1D case it can be observed here as well that with the growth of the number of averaged directional factors the variance of the resultant directional factor decreases.

Conclusion

With simulations for 1 and 2 dimensional regular arrangement antenna systems the developed LRCS theory has been proved. The simulations proved its effectiveness and usability. In the future we would like to do simulations for hardware-realizable LRCS. We would like to determine numerically the RCS reduction factor for standard surveillance radars. Further examinations are necessary to determine the usability of non-regular antenna structures in LRCS systems.

Acknowledgements

This work was supported by the Technology Agency of the Hungarian Ministry of Defence .

Dr. Sipos Mihály:

Jelenkori elektronikai iparunk főbb ökonómiai és geográfiai változási tendenciái

Elektronikai ipar elnevezés alatt a technikai haladás élvonalához tartozó, *analóg és digitális adatokat, mennyiségeket érzékelő, továbbító és feldolgozó infokommunikációs és mérés-technikai eszközöket* produkáló ágazatot értem. A DL statisztikai ágazati kódú *villamos gép, műszer gyártása* (és ezek *javítása*) fogalmi körbe tartozó tevékenységek közül nem tartozik tehát e fogalomkörbe a TEÁOR 31-ba sorolt kábel-, akkumulátor-, világítóeszköz-, villamosmotor gyártás. Az értékelések ennek, valamint az elemzett időszak alatt a statisztikai besorolásban bekövetkezett változások figyelembe vételével készültek. A térképeken mindenkor a nagyobb, jelentősebb termelőcégek elhelyezkedését érzékeltetem.

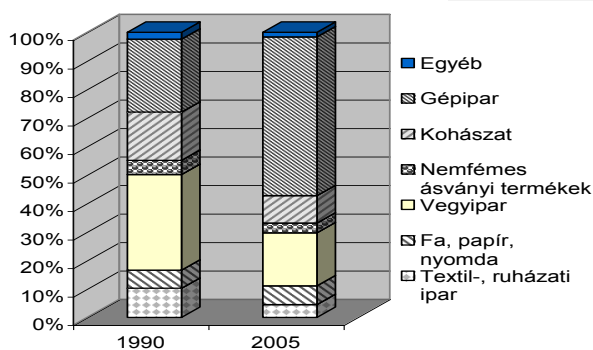
1.) Bevezetés

Az 1970-es évek két *olajválsága*, a rövid idő alatt sokszorosára növekvő kőolajárak elindítójává váltak az olcsó energiahordozókra épített világgazdaság *strukturális válsága* kialakulásának. Mivel az *elektronikai cikkek* gyártásának kicsiny a nyersanyag- és energiaigényessége, a termékek könnyen szállíthatók, ugyanakkor – különösen az új termékfeleslegek – nagy szellemi hozzáadott értéket testesítenek meg, az iparág fejlesztése a nyersanyagban szegény, iparilag fejlett országok számára a krízisből való kitörési pontként jelentkezett. Ezzel a legújabb kori tudományos-technikai forradalom új korszakába érkezett.

Hazánkban az elektronikai ipar a rendszerváltást megelőzően is fontos iparág volt, azonban a kor politikai-gazdasági viszonyai miatt nem voltunk képesek beintegrálódni a világfolyamatokba. A *bekapcsolódás* csak az *1989. utáni* változások hatására *vált lehetővé*. Ugyanekkor a világgazdaság egy átmeneti visszaesése után az elektronikai termékek iránt *növekvő érdeklődés* volt megfigyelhető. A főbb befektetők az Európai Unióból jöttek, aminek a földrajzi közelségen túl a már korábban is meglévő gazdasági kapcsolatok megléte volt az oka: az egyre drágábban gyártó EU-s gazdaság versenyképességét csak a termelésnek az alacsonyabb bérű országokba történő kiszervezésével voltak képesek növelni (1. táblázat). [8]

Ez azt eredményezte, hogy bár az ezredforduló idejére az EU gazdasága egyre jobban lassult, az új demokráciáké, és köztünk a miénk, fokozatosan bővült. Ez együtt járt termelési szerkezetünk átalakulásával. Az ezredforduló utáni, napjainkra is jellemző ipari struktúrát az 1. ábra mutatja be. [8]

1. táblázat A magyar elektronikai ipar külkereskedelmi forgalma országcsoportonként, 2003 (%)		
Országcsoport	ex- port	im- port
EU	81	35
Kelet-Közép-Európa	6	5
Többi fejlett ország	6	18
Fejlődő országok	7	42
Összesen	100	100



1. ábra Feldolgozóiparunk szerkezetének átalakulása 1990-2005 között

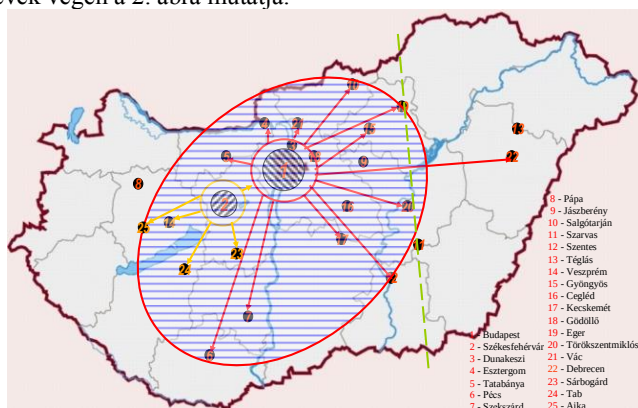
E változások eredményeként az ezredfordulóra Magyarország az EU 9-10. legnagyobb elektronikai gyártójává vált, több mint 2%-kal részesülve az EU termeléséből [5]. Nincs még egy másik olyan iparág hazánkban, amely ma ilyen teljesítményre lenne képes. Ezért is érdemes áttekinteni azokat az okokat és következményeket, amelyek a fenti tények mögött állnak.

2. Elektronikai iparunk a rendszerváltás idején

Hazánkban az elektrotechnikából kialakult elektronikai ipar területi fejlődését – ugyan más-más okok miatt – mind az első világháború előtt, mind azután a Budapest központúság jellemezte, ami tükröződött a második világháborút követő tervutasításos gazdasági rend iparági térszerkezetében is. Az 1960-as évek végétől a fővárosban jelentkező munkaerőhiány az új ipari beruházásokat a munkaerőben akkor még gazdag területekre, az Alföld és a Dunántúl kevésbé iparosodott térségeire orientálta. Az extenzív fejlesztés eredményeként megjelent kisebb-nagyobb vidéki telephelyeken inkább alacsony hozzáadott értékű, alacsonyabb szintű gyártási tevékenységet folytattak. A végtermék

összeállítása, a K+F a budapesti központban folyt. (Az ekkor kialakult *részleg-ipar* vált a rendszerváltás utáni gazdasági válság első számú áldozatává, amikor is eltűnt az elmaradott térségekbe telepített ipari vállalkozások többsége [3].)

Az 1970-es évektől a népgazdaságon belül egyre jelentősebbé vált az elektronikai ipar, ami magával hozta Budapest hegemon központi szerepének gyengülését is. Bár a Videotonban már 1955-ben elkezdődött a rádió-vevőkészülékek sorozatgyártása, azonban nemzetközileg is jelentős, több telephelyes vállalattá csak ekkor nőtte ki magát és tette Székesfehérvárt az iparág második magyar központjává. Az iparág főbb termelőcégei területi elhelyezkedését az 1980-as évek végén a 2. ábra mutatja.



2. ábra Elektronikai iparunk területi jellemzői a rendszerváltás idején

Az 1980-as évtized végére az iparágat tehát egy kettős centrumú struktúra jellemezte. Az egyik az ipartörténeti örökséget tükröző Budapest és agglomerációja az ő vidéki, főleg középüzem szintű telephelyeikkel. Az egyes (vidéki) telephelyek függőségét, alárendeltségét a központtól az ábrán nyilakkal mutattam. Szélsőséges példaként lehet említeni az esztergomi Labor MIM és a Granvisus esetét: csak a vállalati központ, az igazgatói irodák voltak Budapesten, maga a gyár vidéken volt. A térképen jól láthatók a központi ipartelepítési akarat megnyilvánulásai: ott is jelen voltak a szakmakultúra reprezentánsai, ahol a terület természetföldrajzi adottságai elméletileg más iparágak – pl. bányászat és a rá települő nehézipar, energetika – kialakulásának kedveztek (csak a példa kedvéért: Pécs – Mechanikai Laboratórium, vagy Tatabánya – BHG).

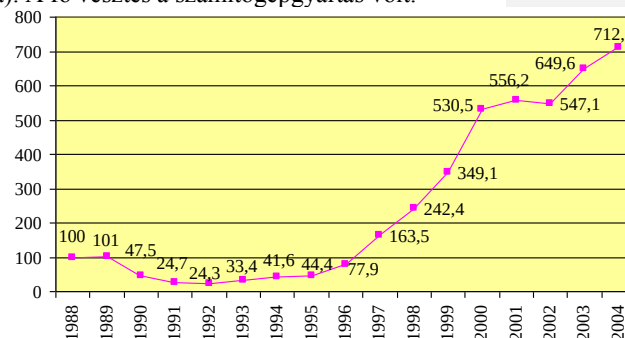
A másik, jóval kisebb hatású (és ezért kisebb körrel jelölt) Székesfehérvár és környéke, amely kapcsolatrendszer a budapestihez hasonló okoknál fogva jött létre. Jellemző, hogy a VT is szükségesnek tartotta budapesti irodák létrehozását. Ezen kívül az országban szétszórva megtalálható még néhány, rész-

ben a II. világháború előtt létrejött cég, részben a hadiipari konverzió miatt polgári termékek gyártására átalított vállalat.

A 2. ábrán megfigyelhető, hogy az ipar az ország középső harmadán koncentrálódott, illetve az Eger-Szarvas vonalnál keletebbre gyakorlatilag nem terjedt ki. Egy további különös tény: Esztergom és Salgótarján kivételével nem találunk a határ közelébe telepített, említésre méltó nagyságú vállalatot. Különösen szembeötlő a *hiányuk a nyugati határvidéken*.

3. Az iparág az átalakulási válság idején (1990-1992)

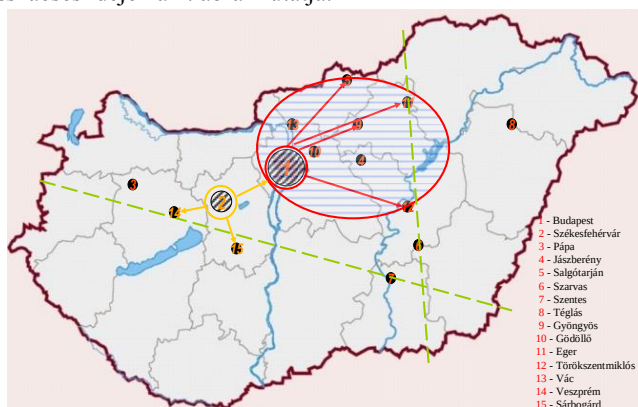
A rendszerváltást követően a magyar gazdaság általános krízise, a belső piac beszűkülése és a hagyományos külső piacok megszűnése, az import liberalizálása, a tőkehiány stb. miatt az iparág *súlyos veszteségeket szenvedett el*. Erre az időszakra az iparág termelése kevesebb, mint a negyedére zsugorodott össze (3. ábra). A fő vesztes a számítógépgyártás volt.



3. ábra Elektronikai iparunk termelési indexének változása 1988-2004 között

Legelőször a kisebb szellemi és pénztőkével rendelkező, *alacsonyabb technológiai szintet* képviselő *vidéki gyártóhelyek*, részlegek zártak be. Ezek jellemzően a Budapest központú nagyvállalatok székhelyen kívüli telephelyei voltak. A visszaesés a nem szerves fejlődés által iparosított térségekben (Észak-Magyarország, Alföld, Közép-Dunántúl) volt a legnagyobb. Az események eredőjeként csökkent a magas műszaki igényességgel jellemezhető termelés súlya, nőtt a tőkeigényes, alacsony feldolgozottságú aránya. Kedvezőtlenül alakult az exportstruktúra, a kényszerű piacváltást nem kísérte termékváltás. A külföldi működő tőke iparági volumene még nem volt jelentős egyrészt a rövid időtáv miatt, másrészt mert *maga a világgazdaság is egy kisebb recessziót élt át* [2].

1992-re az, amit magyar elektronikai iparnak nevezett a statisztika, nem volt más, mint maradvány- és törmelék vállalatoknak napi túlélési gondokkal fenyegetett, vegetáló konglomerátuma [12]. Az iparág területi jellemzőit a gazdasági visszaesés idején a 4. ábra mutatja.



4. ábra Az iparág 1992-93-ban

A recesszió következményeként tovább csökkent mind Székesfehérvár, mind Budapest súlya, összezsugorodott az a kör, amely e két centrum vonzáskörzetét jelentette. A Videoton csödközeli helyzetbe került, több telephelyen leálltak a termeléssel. A budapesti központ szerepe tovább mérséklődött, a térkapcsolatok oldódtak, egyre kisebbé vált a vállalatközi kooperáció. Sorra mentek tönkre a nagy cégek is: BRG, BEAG, MOM stb.

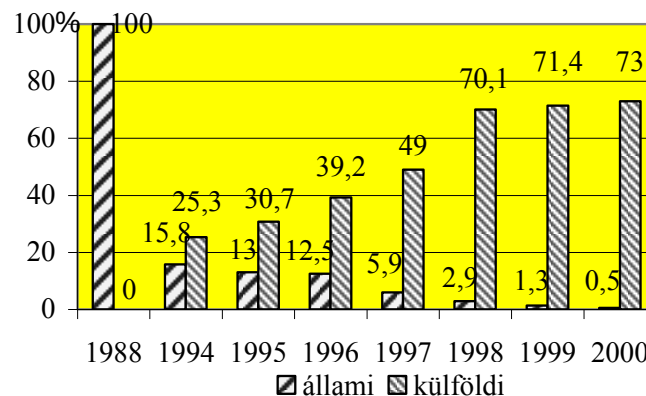
Az 1990-es évek elején szinte teljesen megszűnt Dél- és Délnyugat-Magyarország elektronikai ipara. A néhány túlélő vidéki cég elsősorban a háztartási elektronika gyártói közé tartozott, ami a gyártmányok megfelelően magas műszaki színvonalának, jó értékesíthetőségének köszönhető. Megfigyelhető, hogy nem történt különösebb változás a (tartós állami tulajdonban maradó) védelmi elektronikai cégek esetében (Gödöllő, Törökszentmiklós), ami a ritka kivételt jelentő állami beavatkozásnak tudható be.

A vállalkozások térbeli elhelyezkedésében a továbbra is létező és határvonalat jelentő *Eger-Szarvas vonal mellett* megjelenik egy újabb, kelet-nyugati irányú *Veszprém-Szentes tengely* is, amelytől délre már csak egy-két (elsősorban elektrotechnikával foglalkozó) cég található. Összességül elmondható, hogy a korábbi évek vonatkozásában megfigyelt földrajzi kiterjedés töredékére koncentrálódott az iparággal jellemezhető terület (ld. satírozás).

4. A válságból való kilábalás és az erőgyűjtés évei (1993-1995)

Az iparági output visszaesése 1992-93-ra megállt, amit egy enyhe növekedéssel jellemezhető pár éves időszak követett (3. ábra). A mélypont után, az új gazdasági rend alapjainak lerakásával *elkezdődött fejlődési folyamat* az elektronikai ipar teljes *termelési és területi szerkezetének átalakulását* hozta magával. A *világgazdaság* újra bővülni kezdett, az elektronikai cikkek iránt fokozódott a piaci kereslet. Ennek a *konjunktúrának* köszönhetően nőttek a *külföldi direktinvestíciók* az iparágba, aminek következtében *megváltozott a tulajdonosi (és termék) struktúrája*.

1994-et megelőzően a KSH nem közöl adatokat az egyes iparágak jegyzett tőkéjének illetőségére vonatkozóan. Az 5. ábrából azonban jól látható, hogy a rendszerváltáskor elkezdett privatizáció nagy léptekkel haladt előre az elektronikai iparban: az elemzett időszakban az állami tulajdon részaránya már 16 % alá csökkent, a külföldi pedig 25% fölé nőtt. Pártpolitikai színezettől függetlenül érvényesült a továbbiakban is a feldolgozóipari állami tulajdon lebontásának elve, ami az ezredfordulóra gyakorlatilag el is érte célját. Ezzel egyidőben a külföldi működő tőke részaránya 72-73% körül állandósult.

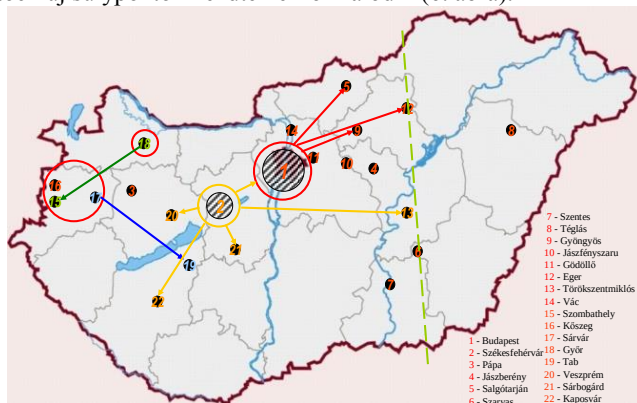


5. ábra Az állami és a külföldi tulajdon részaránya a jegyzett tőkén belül az elektronikai iparban

Ezeztől az évektől kezdve a *korábbtól eltérő ipartelepítő tényezők* válnak uralkodóvá. Mivel jellemzően mind az itt felhasznált nyersanyagok, mind a késztermékek súlya relatíve alacsony, viszont áruk magas, ezért a vízi, vagy vasúti helyett a legjellemzőbb szállítási mód a közúti (autópálya), esetenként a légi. A természeti tényezőktől kevésbé függ, ezért viszonylag széles földrajzi határok között művelhető. A gyártási technológiához tartozó esetenkénti szigorúbb tisztasági, hőmérsékleti feltételek könnyen betarthatók. Ezzel szemben fokozottabb követelményeket támaszt a munkaerő képzettségi szintjével és a jó minőségű műszaki infrastruktúrával szemben. Ez utóbbiak közül kiemelen-

dő a jó infokommunikációs szolgáltatói háttér, a gyors határátlépés feltételeinek biztosítása, a zavartalan elektromosenergia-ellátás.

Az előző rendszerből örökölt és az új technológiák közötti *barrier leküzdésére* az új, zöldmezős beruházások ígérték a legjobb megoldást. A befektetők speciális érdekei érvényesülése következtében az iparág földrajzi elhelyezkedését illetően új súlypontok kezdtek el formálódni (6. ábra).



6. ábra Az iparág új központjai megjelenése 1995-96-ban

A külföldi és hazai *beruházók* meghatározó módon a *piaci viszonyokból* indultak ki, az *állami akarat* ebbe a folyamatba *csak kis mértékben avatkozott* be – pl. a távközlés fejlesztéséhez kapcsolódó, akkor még állami beruházások esetében a szállítók számára előírta a minimális magyar résztulajdon hányadot, ezzel próbálva elősegíteni az egyes cégek túlélését, ami talán csak a Telefon-gyár esetében sikerült. Ekkortájt kerültek felszámolásra az olyan nagyvállalatok, mint a BHG, Gamma, FMV.

A *nyugati határ közelében* a külföldi tőkebefektetések révén, zöldmezős beruházások formájában, új vállalkozások jelentek meg. Olyan városokban, ahol gyakorlatilag nem volt jelen az iparág, új elektronikai termelő cégek alakultak. A helyválasztás okai között ekkor még a nyugat-európai felvevő piac közelsége dominált, azonban fontos szerepet játszott a már meglévő M1 félautópálya és a magyarországi átlagnál jobb állapotú távközlési infrastruktúra is. *Szombathely központtal* egy új, kisebb ipari *centrum csírája* bontakozott ki. Ebbe a körzetbe tartozik Sárvár is, ahol a Flextronics alapított új céget, mit egy újabb gyár követett Tabon. A Philips gyára révén *Győr* is bekapcsolódott a folyamatba – a holland cégnek mindkét városban volt már ekkortájt üzeme.

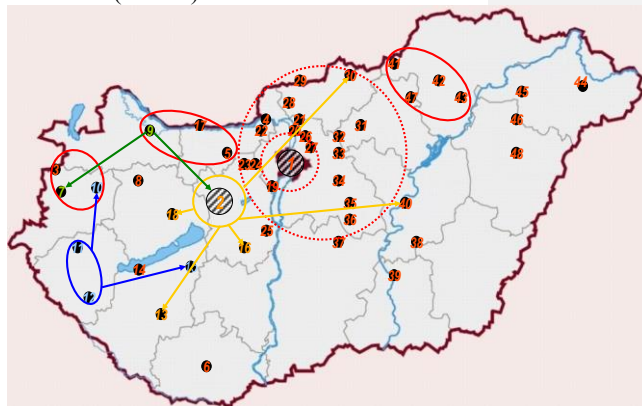
Budapest tovább marginalizálódott: a megszűnő korábbi nagyvállalatok helyett újak gyakorlatilag nem jöttek létre, a vidéki telephelyek az eltűnő központtól immár teljesen függetlenné váltak. Részben a fővárosfejlesztési kon-

cepcióknak köszönhetően itt az ipar helyett ekkor már a szolgáltatások erőteljes bővülése jelentette a fő hajtóerőt. Az 5. ábrán ezt a folyamatot a kapcsolatrendszer bemutató nyílak számának csökkenése érzékelteti. A másik régi centrumot fémjelző Videoton viszont kezd *megújulni*. Egyre ígéretesebbé vált az EMS tevékenysége, ami a vidéki telephelyek újbóli életre keltéséhez is alapot biztosított – ld. az újra bővülő VT-kapcsolatrendszert. Pozitívum továbbá, hogy a kevés számú, mélypontot túlélt, magyar kézben lévő jelentős vállalkozás helyzete stabilizálódott, sőt néhányuk revitalizálódott.

5. Az iparág a nemzetgazdaság hajtómotorjává válik (1996-tól napjainkig)

Az 1990-es évtized első felében gyors jövedelmi, fejlettségi polarizáció tanúi lehettünk minden szinten, majd néhány év múlva *stabilizálódtak az egyenlőtlenségek*. 1995-96-tól kezdve megjelentek a megújulás makrogazdasági jelei, a regionális sikerek új csomópontjai, vagyis a *növekedésnek indult gazdaság* az ágazati differenciálódás mellett *földrajzi területenként is eltérően fejlődött* [6]. 1996-tól kezdve az iparágban *óriási pozitív változások* történtek. Az új telephelyek szinte robbanásszerűen jelentek meg és terjedtek el az országban, a termelés soha eddig nem látott volument ért el. Az *újonnan létrejött ágazati térszerkezet* gyökeresen *különbözik* a korábbiaktól: a vizsgált iparág területi elhelyezkedése kiegyensúlyozottabbá, *összetettebbé* vált.

Az 1990-es évtized közepétől az immár végleges politikai változások, az egyre jobban stabilizálódó gazdaság, a bevezetett állami adókedvezmények kifejezetten *ösztönzően* hatottak a *külföldi direktinvestíciókra*. Ennek következtében a vizsgált periódus végére az elektronikai ipar teljesen megújult és az egyik legfontosabb iparaggá vált hazánkban [7]. *Területi elhelyezkedése egyenletesebbé* vált (7. ábra).



7. ábra Az iparág megújult térszerkezete

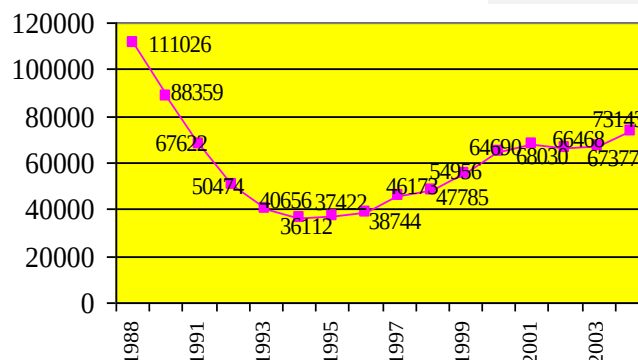
Az ország legnyugatabbi területein a legnagyobb befektetők *több telephelyes struktúrát* hoztak létre, igyekezve maximálisan kihasználni a helyi lehetőségeket: a kedvező szállítási körülményeket, a munkaerő kínálatot, az adókedvezményeket. 2000-re saját hálózatot, munkamegosztási rendet alakított ki a Philips, a Flextronics, a Videoton.

Az iparág fokozott jelenléte leginkább a Nyugat-Magyarországi Régióban, illetve a *Budapest-Győr növekedési tengely* mentén érzékelhető, ahol két regionális csoportosulás is kialakult. Az egyik Szombathely körzete, ahol két, többtelephelyes hálózatot kiépítő multi is megjelent, a másik maga az *M1 autópálya nyomvonala*. Komárom, az ottani ipari park önmagában is jelentős termelési tényezővé nőtte ki magát (Nokia és beszállítói), de a Philips révén Győr is szót érdemel.

A Közép-Dunántúlon elsősorban a *Budapest-Székesfehérvár-Nagykanizsa tengely* (azaz az M7-es nyomvonala) emelendő ki. Ennek déli végén a szingapúri bejegyzésű Flextronics gyárai találhatók, a középső területen a Videoton érdekeltségei, északon pedig a budapesti agglomeráció. Az egyetlen, európai viszonylatban is jelentős magyar tulajdonú cég, a Videoton az 1990-es évtized közepén túljutott a krízisen. Az új tulajdonosi és cégvezetői kör az önálló termékek helyett az EMS profilú tevékenységbe kezdett, ami egyre eredményesebbé vált. Ez sikeresen elvezetett a cég vidéki telephelyeinek reaktivizálásához, a térbeli kapcsolatok újjászűléséhez, kialakítva egy új vállalatbirodalmat.

Az évtized végére e térségekben nagyon lecsökkent a szabad munkaerő nagysága, ezért az iparág nyugat-magyarországi bővülése a *foglalkoztatottsági problémákba ütközve lelassult*. Itt figyelembe kell venni, hogy a magyar munkaerő csak kevésbé mobil, amiben szerepet játszanak a felnőttképzés hiányosságai, a depressziós területek eladhatatlan lakóingatlanai, háztáji telkei, az évtizedes megrögzöttségek stb. Ezért Nyugat-Magyarországon több helyen külföldi állampolgárokat is alkalmaznak.

Továbbra is *kihasználatlanok* viszont a *délnyugati megyék* munkaerő tartalékai. Itt az ipar csak a délszláv háború elültével erősödött meg, a térség iránti bizalom növekedése nagyban betudható hazánk NATO békepartneri státuszának, majd tényleges taggá válásának. A térség legnagyobb elektronikai cégei már 1995-96-ban megjelentek (ld. Nokia, Elcoteq Pécssett), azonban a további jelentős investíciók mind a mai napig váratnak magukra. Az iparágban foglalkoztatottak létszámának alakulását a 8. ábra mutatja be [8].



8. ábra Az iparágban foglalkoztatottak számának alakulása, 1988-2004 között

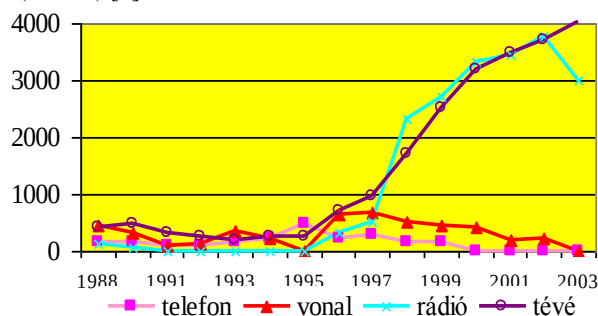
Ugyanakkor több olyan multinacionális cég is volt, amely nem félt átlépni a Duna vonalán, így az évezredforduló tájékán elindult egy (észak)kelet-magyarországi terjeszkedés is. A főváros körül kialakult egy vállalati gyűrűrendszer, melynek belső sugara ténylegesen Budapest középpontú, azonban a külső határvonalé már jóval keletebbi. A fővárosban alig egy-két régi cég maradt, újak nem települtek, az ipar jelentősége lecsökkent, helyét a *tercier szektor* vette át [3]. Az új vállalkozások a *tágabb agglomerációt választják*, ahol lényegesen alacsonyabbak a telekárak és az iparüzési adó mértéke. E folyamatra kitűnő példa az M1-M7 Budapestre bevezető szakaszánál lévő Budaörs. Ezzel szemben a hasonló adottságú budapesti külső kerület részeket a régi gyártelepek lepusztult romjai jellemzik. Egyetlen örvendetes tény, hogy a Magyarországon megvalósult kevés számú K+F beruházások zöme itt jött létre.

Kelet-Magyarországon az új elektronikai (multinacionális) vállalkozások többsége csak 1999-2000-tól kezdve jelent meg. Ennek legfőbb oka a *hiányos infrastruktúra*: az M3-as gyorsforgalmi út a tanulmány írásakor még mindig nem kötötte be az ország vérkeringésébe a térség legnagyobb városait (Debrecen, Nyíregyháza) és Miskolcra is csak 2004-ben ért el. Így közöttük még nem tudtak kialakulni erős belső kapcsolatok [10]. Azonban már az a tudat, hogy az autópálya a közeli jövőben elér ezen települések közelébe, önmagában is elegendő volt ahhoz, hogy a tőke beáramlása e térségbe megnöjjön. Így alakult ki pl. maga a miskolci körzet is.

Másik meghatározó tényező a *feldolgozóipari tapasztalatok hiánya*. A Borsodi-medence kivételével *számottevő ipar korábban sem volt*, a dolgozók az ország más területein próbálkoztak munkát találni – általában az alacsonyabb szakképzettséget igénylő munkakörökben. Mivel az ipar átstrukturálódását nem kísérte a dolgozók tömeges átképzése, ezért a munkanélküliek foglalkoztathatósága komoly problémákba ütközik, ami Észak- és Kelet-

Magyarországon depressziós körzetek kialakulásához vezetett. Pozitívumként meg kell említeni, hogy mind a központi, mind a helyi (ön)kormányzatok *direkt ösztönzőkkel* – adókedvezményekkel, munkahelyteremtő támogatással stb. – igyekeztek az *FDI figyelmét e térség felé* terelni [4].

A magújult tulajdonosi kör új technológiákat, gyártmánystruktúrát is hozott magával. Míg 1990. előtt jelentős volt a professzionális elektronikai termelés részaránya, mára a szórakoztató elektronika, a perszonális híradástechnikai eszközök termelése jelenti a többséget. Ezt a folyamatot négy termék példáján érzékeltetem (9. ábra) [8].



9. ábra Néhány elektronikai termék gyártásának alakulása

Mint látható, a szórakoztató elektronika előállítását a hazai távközlő hálózat kiépülésével párhuzamosan fokozatosan átvette a professzionális termékek helyét a gyártmánystruktúrában. Sajnálatos módon a talán legnagyobb volumenben előállított mobil telefonok mennyiségéről a gyártó(k) titkolózása miatt nincs számszerű információ.

A KSH adatai alapján felrajzolhatók az *ideáltipikus elektronikai vállalkozás* fő jellemzői. A tulajdonosi struktúrára a magántulajdon, a vállalatméretre a dualitás a meghatározó. A legnagyobb számban lévő, *magyar tulajdonú* cégek túlnyomó többsége a *KKV kategóriába* tartozik és elsősorban belföldi igényeket elégít ki. Társasági formája elsősorban Bt vagy Kft, de jelentős az egyéni vállalkozók száma is. Sokkal kevesebb a gyakorlatilag *kizárólag exportra* termelő, *külföldi tulajdonban* lévő, a nagy-közepes, illetve *nagyvállalati kategóriába* sorolható cégek száma, azonban ezek hatása a nemzetgazdaság eredményeire lényegesen nagyobb. Többségük Kft-ként működik, de található néhány Rt is közöttük.

6. Napjaink néhány makrogazdasági problémájának vetülete az iparágra

Az elmúlt 16-17 év alatt a magyar elektronikai ipar tulajdonosi köre, technológiája, termékei, piaci orientáltsága gyökeresen megváltozott, a gyártás új

telephelyeken, a régítől eltérő geográfiai eloszlásban folyik. Ugyanakkor ez a megújulás kívülről vezérelt, mivel az iparág önálló megújításához nem rendelkezünk elegendő forrásokkal. Az *exogén technológiai fejlődéssel* történő felzárkózás Magyarország számára gyors, látványos eredményt hozott: jellemző módon a feldolgozóiparunkban előállított javak egyötöde itt jön létre, hazánk eredményesen integrálódott termelőként az iparág globális termelési hálózataiba. Ez azonban *veszéllyel is jár*. Ha az iparágban nem indul el olyan gyors technológiai képesség-felhalmozás, amely minőségi továbblépést, vagyis a fajlagos hozzáadott érték adott iparágon belüli növekedését teszi lehetővé, a makro-mutatók látványos javulása konjunkturális eredetű marad: megállhat, sőt, visszajára is fordulhat [9], [11]. Erre már volt is példa az elmúlt években.

Hazánk még mindig a beruházáson és technológiaiimporton alapuló fejlődési szakaszban van. Nemzetközi versenyképességünk a tömegtermékek és szolgáltatások előállításának hatékonyságán múlik. Idővel ugyan növekedett a hazai hozzáadott érték aránya, de a termékkonstrukciók és a termelési eljárások nem hazaiak. A továbblépés feltétele a hazai termék- és technológia-fejlesztési képesség kialakítása. A kormányzat szerepe ebben a folyamatban a beruházási környezet ápolása, vonzóvá tétele, aminek révén fokról-fokra erősödhetnek a vállalatok technológiafejlesztési, piaci innovációs képességei [1].

Nem szabad elfelejteni, hogy a nemzetközi vállalatok számos telephely közt választhatnak, a kormányok versengenek a külföldi beruházásokért, a vállalat-specifikus versenyelőnyök viszonylag könnyen áthelyezhetők egyik országból a másikba (ld. IBM profil eladásai a kínai Lenovónak és a japán Hitachinak). Másfelől növekedett az olyan „mesterségesen létrehozott” erőforrásoknak a jelentősége, mint például a szakképzett munkaerő, a műszaki hozzáértés, vagy a vállalati általános költségekbe sorolható (irányítási, marketing, szállítási, jogi, logisztikai, stb.) funkciók. A makrogazdaság-politikai mozgástér beszűkülése nem jelenti tehát a közsféra gazdaságpolitikai szerepének csökkenését.

A fejlett technológia importján és hatékony termelési, vállalatirányítási eljárások alkalmazásán alapuló fejlődési szakaszból az *innovációs tevékenységeken (tudáson) alapuló fejlődésre való áttéréshez* továbbra is szükséges a kormány aktív szerepvállalása. Ennek eszközei egyebek mellett: állami támogatás a magánszektor K+F-tevékenységéhez, a felsőoktatás fejlesztéséhez, valamint a magas technológiai színvonalú induló vállalkozásokhoz.

A 7. ábrán jól látható, hogy a délkeleti, keleti határaink mentén az iparág nem tudott érdemben megkapaszkodni – sőt az Eger-Szarvas vonal is érzékelhető mind a mai nap. Szakképzett munkaerő hiányában nem is várható, hogy belátható időn belül ezeken a területeken elektronikai gyártás jöjjön létre. Mivel a magyar munkaerő (többek között a magas munkabérek és a hozzájuk kapcsolódó terhek miatt) egyre kevésbé versenyképes, ezért nem lehet figyelmen kívül hagyni a *cégek kivonulásának lehetőségét*. Például, a logisztikai, pénzügyi és egyéb tényezők összevetéséből származó indexszámok szerint

2008-ra a nagy élőmunka-igényű termelés számára Magyarország feleannyira lesz vonzó, mint Szófia környéke – feltéve, hogy Bulgáriában tovább épülnek az autópályák. Itt figyelembe kell venni még azt is, hogy az egy főre jutó átlagos feldolgozóipari munkaerőköltséggel kalkulálva egy német munkahely Magyarországra kerülésekor, az ottani 2000 eurós havi bér helyett csak 500 eurót kell kifizetni, egy magyar gyár Romániába telepítésén csupán 250 euró/főt lehet spórolni, amit az ott még *meglévő logisztikai problémák Magyarország javára ellensúlyozni tudnak*.

Az uniós támogatással épülő *transzkontinentális autópálya-hálózat* Magyarország javára megváltoztathatja a jelenlegi *logisztikai csomópontokat*. A közúti közlekedés kiépülése után a Távol-Kelet és Európa gyárai között hajózó elektronikai alkatrészek és késztermékek Rotterdam és Hamburg helyett két nappal hamarabb a romániai Constantába és a szlovéniai Koperbe érkezhetnek, ami javíthat hazánk pozícióin. Azonban figyelembe kell venni azt a tényt, hogy az autópálya megléte önmagában még nem jelent semmit: nem képes dinamizálni a környezetét, ha nincs mit [13].

Azok a cégek, amelyek hosszabb távú stratégia keretében döntöttek magyarországi megjelenésükről és kelet-közép-európai régióközpontot építettek ki nálunk, illetve kutató-fejlesztő bázist is kialakítottak, vélhetően nem csökkentik magyarországi aktivitásukat. Azonban egy újabb látványos felfutás – figyelembe véve az anyavállalatoknál erősödő szakszervezeti és társadalmi ellenállást, az európai részvénytársaság intézményének létrejöttét – nehezen valószínűsíthető.

Irodalom:

- [1] ALTENBURG T. (2001): *Ausländische Direktinvestitionen und technologische Lernprozesse in Entwicklungsländern* – In: Geographische Rundschau, Berlin; Vol. 53 No. 7-8. pp. 10-15.
- [2] BARKÓ J. – SIPOS M. (1992): *Kell nekünk elektronikai ipar?* – Ipari Szemle, 5. pp. 16-18.
- [3] BARTA GY. (2002): *A magyar ipar területi folyamatai 1945-2000* – Dialog-Campus Kiadó, Budapest-Pécs, p. 272.
- [4] CZABAN, L. – HENDERSON, J. (1998): *Globalization, institutional legacies and industrial transformation in Eastern Europe* – In: Economy and Society, London, United Kingdom. Vol. 27, No. 4. pp. 585-613.
- [5] *European Business. Facts and Figures Data 1988-2002*. Eurostat, Luxembourg p. 422
- [6] HORVÁTH GY. – RECHNITZER J. (2000): *A külföldi működő tőke szerepe a magyar ipar duális struktúrájának és regionális differenciálódásának kialakulásában* – Magyarország területi szerkezete és folyamatai az ezredfordulón, MTA RKK, Pécs, p. 282.

- [7] LAJTHA GY. (1999): *A hazai távközlési ipar* – Magyar Tudomány 44. évf. 9. szám pp. 1079-1090.
- [8] *Magyar Statisztikai Évkönyvek 1988-2004*. KSH, Budapest
- [9] PIANTA, M. – MELICIANI, V. (1996): *Technological specialization and economic performance in OECD countries* – In: Technology Analysis and Strategic Management, Manchester, UK. Vol. 8 No /2 pp, 157-174.
- [10] SIPOS M. (2004): A magyar elektronikai ipar átalakulása 1990-2000 között In: PITRIK J. – ULCZ GY. (szerk.): Társadalmi-gazdasági mozaikok az uniós kapcsolatok tükrében – Pécs-Szeged, pp. 143-172.
- [11] SZALAVETZ A. (2004): Technológiai fejlődés, szakosodás, komplementaritás, szerkezetátalakulás. Külgazdaság, 2004. április pp. 362-378.
- [12] SZENTGYÖRGYI ZS. (1994): *A magyar elektronikai ipar összeomlása Okok és következmények* – Magyar Tudomány 39. évf. 5. sz. pp. 573-587.
- [13] TÓTH G. (2005): *Az autópályák szerepe a regionális folyamatokban* – KSH, Budapest p. 128.

Attila Takács

New challenges in the area of European electronic government

1. Revaluation of the process of the European eGovernment

Nowadays the policies of the eGovernment of the members of the European Union are characterized of revaluation. The change has three types:

- a) The EU settles concrete projects beside and instead overall developmental policy for the memberships.
- b) Strengthen the movement towards a model which is characterised as a thing beside the client centralized strategy and the interoperability among the organs of the civil services.
- c) The eGovernment as the pledge of technological change and competitive. And finally it can be an active supplying state.

It won't be the most important thing that we can access everything online. The most important that nobody will be preclude the possibility of using ICT equipment in every member state.

2. Electronic government on supranational level

The establishment of the eGovernment in the EU was caused by the ambitions for the political power over every nation and the leader position in the world in the economic and financial relation. We could observe a paradigm change in the time of Barroso committee. This change affect the territory of eGovernment. In influential European circles opinion the reach of the Lisbon's targets isn't possible⁷³ for 2010. Therefore initiating of the new targets and priorities initiating are hurried as new radical structural reforms. The program of Commissioner⁷⁴ for Information Society and Media contains the following summarized points:

- a) Information field in Europe without borders,
- b) ICT based investment and innovation,
- c) Social reception and creating a higher quality life.

The most important thing of the building of the most competitive knowledge based society to develop the online civil services which demand the cooperation of the member states. The Commissioner said that the keys to the realization of eGovernment were the followings:

- a) identification Management,

⁷³ instead of vision of the most competitive knowledge based society and economy in the word

⁷⁴ Viviane Reding's 3rd program

- b) interoperability between systems,
- c) spreading of the best practices,
- d) development of the Pan European services and powerful operate.

3. Result of the eGovernment development in the EU nowadays

Success of the supranational eGovernment policy depends on two fundamental factors. Partly the EU has to dispose of professional political system resources to develop the electronic government, partly reasons have to be mapped which led to the form of the divided Europe and result in no operative work in eGovernment. The EU showed significant leap forward in the professional political system resources. Partly it has overall strategy, partly the Union starts to use the devices of the different areas⁷⁵ and starts constitutional changes with the help of ICT technologies.

The success of the supranational eGovernmental performance is endangered by the divided Europe and the unlevelled development. The cause and effect of the different performances are the followings:

- a) The performance of the e-services show close connection with the GDP and the economic competitive. In those countries where the GDP is very high, there is eGovernmental strategy, there are correct online services and the modernization is done by an independent establishment in the hierarchy of the ministry the performance is higher. In the poorer countries the area of the eGovernment hasn't independent priority, this is only the part of the realization of the information society and the level of the online services is lower than in the modern countries.
- b) The performance of the eGovernment is closely connected with spreading of internet. If the online e-services are correct in a country then usually the level of the informational literacy is very high.

4. Aspirations in the EU eGovernment

The aspirations of the EU eGovernment started in 1995 in the scope of IDA⁷⁶ program. The IDA is responsible for the most important processes in the eGovernment and the IDA coordinates the highest European level the back-office processes, the standardization and the pan European services. It has two parts: a) 1995-1999, b) from 1999 to this day. The trend of political planning of the eGovernment is attached to the operation of the Barroso committee. The foundations of this operation are the followings:

⁷⁵ essentially: regional policy, internal market, regulation of competition, policy of industry, trans European networks, research + development

⁷⁶ Interchange of Data between Administrations

- a) The modernization of the civil service: the purpose is to make an open and banner civil service that everybody can use democratic foundation.
- b) Innovative governmental services: to create online services (personal, low cost)
- c) To propagate pan European civil service applications: cooperation between the civil service networks.

Inside all of these, in priority of the period of 2006-2010 the next things are formulated in addition to pan European target:⁷⁷

- a) Electronic identification and authentication in the civil services,
- b) European digital nationality,
- c) European interoperability prescriptions,
- d) Strengthen the PPP model,
- e) Examination of the eGovernment social effects, specification of the measuring limits,
- f) Creating the deeper integration between the multi storey eGovernmental services.

Over the general direction in the interest of the reaching the equal eGovernmental advanced state the EU try to formulate concrete projects and unified political attitudes in addition to specification of strategic policy. Recently accepted EU recommendations formulate the following purposes:

- a) To have to reduce with 25% administrative limits towards the citizens and businessmen.
- b) To have to form the methods of the identification and authorization in the use of pan European services,
- c) To have to be realized the civil service without paper,
- d) To have to stimulate the use of eGovernmental services.

The new supranational action plan, which will be valid for 2010, and it is drafted according to CoBrA recommendations, specify the most important milestones in the followings:

- a) It can be reached the use of the electronic identification and authorization system for every people, concern and administrative system in the EU,
- b) It has to be worked out an identification and authorization system for the electronic documents,
- c) It has to be realized the reception for every member of the EU with ICT appliances,

⁷⁷ formulated: eEurope Advisory Group's eGovernment subgroup in the „Working Paper beyond 2005“

- d) It can be reached every public information and services,
- e) it has to be reduced every administration commitment for the citizens, and it has to be established more efficient public systems in favour of transparency and questionability,
- f) it has to be realized super national level services⁷⁸ with wide effect,
- g) it has to be realized the change of the data and interoperability between governments by public standards.

The realization can be helped in the member states by the using of the new governing principles which are required in these countries.

5. Summary

There is no way to execute the plans which were accepted in Lisbon, therefore the change of the paradigm can be observed in the further development of the territory of the eGovernment and eServices. The realization of the new governing principles will be obligatory for every member state. It can be helped by the keeping of the action plan, which was made by the CoBrA recommendations. The potential developmental processes of the eEuropean civil services after 2005 decisively influence the future of the national eGovernment and eServices therefore the further development of the cooperation of the communicational systems of the governmental and defensive area will be defined by the EU conceptions and acquisitions.

Bibliography

- [1] Az elektronikus aláíráshoz és alkalmazásaihoz kapcsolódó monitoring jelentés, GKI Gazdaságkutató Rt. – Nemzeti Hírközlési Hatóság, 2004, http://www.nhh.hu/e_alair2004gki_nhh.pdf
- [2] Broderick, Terry R.: Regulation of Information Technology in the European Union. Kluwer Law International, London, 2000.
- [3] eEurope 2005: An information society for all (An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions), Commission of the European Communities, Brussels, 28. 5. 2002., COM (2002) 263 final, http://www.ihm.hu/tarsadalom/strategia/eeurope2005_en.pdf

⁷⁸ Focused on the realization of the complete eGovernment Procurement

Németh András okl. mk. főhadnagy:

A katasztrófavédelmi kommunikáció alternatív megoldásai

Bevezetés

Vajon a 21. század első évtizedének derekán mi jelenti a legnagyobb veszélyt az emberiségre? Ezt a kérdést egyre gyakrabban tehetjük fel az elmúlt öt évben, hiszen ezen időszak krónikájában számos olyan címszó szerepel, melyek önmagukban is megrengették a világot. Általánosságban elmondhatjuk, hogy az emberiséget fenyegető legnagyobb veszély maga az EMBER!

Az elmúlt száz évben az egymást követő, ipari, technológiai, technikai és információs forradalmak és robbanások, valamint a Föld lakosságának ugrásszerű növekedése élő környezetünk állapotának jelentős romlását eredményezték. Atomrobbantások, erdőirtás, üvegház hatású gázok növekvő kibocsátása, a természeti erőforrások korlátlan kihasználása nagy valószínűséggel jelentős szerepet játszott abban, hogy az időjárás az elmúlt évtizedre drasztikusan megváltozott. Ezen változás megnövelte az extrém légköri jelenségek következtében kialakuló szélsőséges időjárási jelenségek előfordulási valószínűségét a világ minden területén. (Árvizek, elemi erejű szélviharok, szélsőségesen alacsony és magas hőmérsékletek, aszályok, extrém mennyiségű csapadék...) (Természetesen számos olyan természeti katasztrófa is történt, melyek nem elsősorban az emberi tevékenységek következményei: pl.: földrengés, vulkánkitörés, szökőár)

Az ember, mint közvetlen veszélyforrás, a civilizációs katasztrófák (ipari balesetek, terrortámadások) számának növekedésében játszik szerepet. 2001. szeptember 11. Egyesült Államok, 2004. március 11. Spanyolország, 2005. július 7. Nagy-Britannia... Néhány, kifejezetten a nyugati civilizáció ellen irányuló terrortámadás helyszíne, ahol új megvilágításba került a globális biztonság értelmezése. Ez azonban csak a jéghegy csúcsa, hiszen a világ számos országában ezek és ezek hallnak meg fanatikus politikai, vagy vallási félkatonai szervezetek által elkövetett támadások következtében, melyeket vélt, vagy valós sérelmek megtorlásaként, vagy a félelemkeltés eszközeként intéznek a polgári lakosság ellen. A másik fontos veszélyforrást olyan hétköznapi emberi tevékenységek jelentik, mint a szárazföldi-, vízi-, vagy légi közlekedés, ipari és mezőgazdasági termeléshez kötődő tevékenységek, energiatermelés, szállítás stb., melyek következtében bekövetkező katasztrófa-helyzetek valószínűsége, a gyors technológiai fejlődés következtében egyre bonyolultabbá váló infrastrukturális környezet miatt egyre nő. Ugyanakkor egyes fejlődő országokban - ahol az emberéletnek nincs „értéke” - éppen az elavult termelési eljárások jelentik a veszély fő forrását. (Gondoljunk például a Kelet-Ázsiában bekövetkező gyakori bányászercsétlenségekre.)

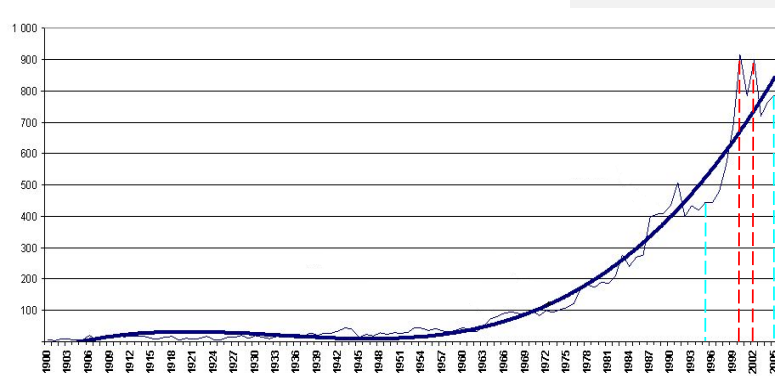
De beszéljünk akár természeti, akár civilizációs katasztrófákról, az ellenük való védekezés, valamint következményeik felszámolásának hatékony-

ságát - sok más tényező mellett - jelentősen befolyásolják a védekezésben résztvevők számára rendelkezésre álló információtovábbítási lehetőségek, kommunikációs rendszerek.

A fentiek alapján tehát először azt érdemes megvizsgálni, hogy világszerte milyen tendenciát mutat a katasztrófák, az érintett lakosok, valamint a halálos áldozatok száma, ezáltal igazolva a katasztrófavédelemmel kapcsolatos tevékenységek egyre növekvő jelentőségét. Ezt követően a védekezési munkálatok tervezése, szervezése, irányítása és vezetése szempontjából fontos, a jelen állapotok szerint és a jövőben igénybe vehető kommunikációs infrastruktúrát, azok alkalmazhatóságát és szolgáltatásait röviden összefoglalva teszünk ajánlást egy többszintű rendszer bevezetésére, amely extrém helyzetekben is képes biztosítani magyarországi és nemzetközi viszonylatban a készenléti és együttműködő szervezetek híradását.

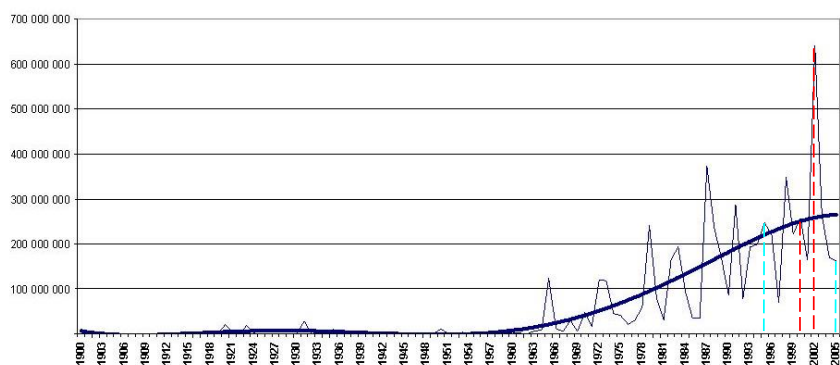
Tendenciák⁷⁹

Az elmúlt valamivel több mint száz év regisztrált katasztrófáinak (természeti és civilizációs) számát ábrázoló diagrammon jól megfigyelhető a jelentős növekedést mutató tendencia, melynek két „kiugrása” (közel 900 jelentős „eseménnyel”) a 2000 és 2002-es évben volt. (Ezt elsősorban a hidrometeorológiai katasztrófák számának drasztikus növekedése okozta.)



1. ábra: A katasztrófák számának változása 1900 és 2005 között
(Forrás: EM-DAT)

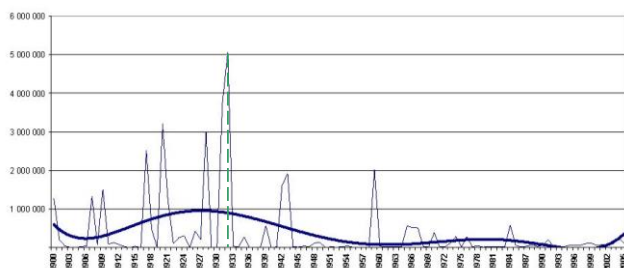
⁷⁹ A statisztikai adatok és diagrammok az 'Emergency Events Database' (EM-DAT) –ból származnak (<http://www.em-dat.net>). Az adatbázis csak olyan eseményekkel számol, amelyek esetében négy feltétel közül legalább egy teljesül. (legalább 10 halálos áldozat; legalább 100 veszélyeztetett/érintett; veszélyhelyzet került kihirdetésre; nemzetközi beavatkozásra volt szükség)



1. ábra: A katasztrófák által érintett népesség 1900 és 2005 között (Forrás: EM-

A 2. és 3. ábrán a katasztrófák által érintett népesség, valamint a halálos áldozatok száma látható.

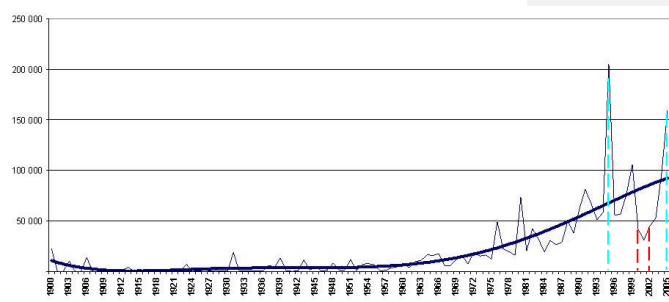
Ami szembeötlő, hogy míg az érintett népesség a katasztrófák számához hasonlóan évről évre növekszik (ez a Föld népességének növekedésével és urbanizációval is magyarázható), addig a halálos áldozatok száma csökkenő tendenciát mutat. Ennek oka a katasztrófavédelmi szervezetek kialakulása, a reagáló-képesség növekedése, a rendelkezésre álló technika és technológia fejlődése, és a tapasztalok rendszerbe történő visszacsatolása, azaz együttesen a megelőzés, védekezés és elhárítás hatékonyságának növekedése lehet. Ezen hatékonyságnövekedés egyik alapvető feltétele a vezetést és irányítást támogató hírközlési infrastruktúra, valamint az igénybe vehető kommunikációs eszközök fejlődése, amely biztosítja a lakossági riasztás rendszerének, valamint a védekezésben résztvevő szervezetek és személyek közötti gyors információ továbbítás feltételeit.



2. ábra: A katasztrófák halálos áldozatai 1900 és 2005 között (Forrás: EM-DAT)

Az érintettek számát tekintve abszolút rekordernek számít a 2002-es év, amikor is számos árvíz és szélvihar pusztított Európában, Észak- és Dél-Amerikában és Ázsiában. A közel 650 millió érintett több mint 95%-a kínai árvizeknek és szélviharoknak, valamint a nagy indiai árvíznek és aszálynak köszönhető. A fenti számot tekintve csodával határos, hogy ebben az évben világszerte „alig” ötvenezeren veszítették életüket valamilyen természeti katasztrófa következtében. (De még az elmúlt húsz esztendő legtöbb, több mint negyedmillió halálos áldozatot követelő 2004-es délkelet-ázsiai szökőár pusztítása is eltörpül a múlt század első felében bekövetkezett természeti csapásai mellett. 1932-ben például 5 millióan haltak éhen a Szovjetunió területén.)

A 4. ábrán a katasztrófák által okozott, 2005-ös árfolyamon számított anyagi kárérték alakulása látható millió amerikai dollárban kifejezve (világviszonylatban).



3. ábra: A katasztrófák által okozott anyagi károk 1900 és 2005 között
(Forrás: EM-DAT)

A fenti ábrán látható ugyan, hogy a katasztrófák számának emelkedését követi az elszenvedett anyagi károk értékének növekedése, egyenes arányosság azonban nem írható fel a két tendencia között. Jó példa erre a 2000 és 2002-es év, amikor is a bekövetkezett 'események száma' kiugró volt ugyan, az okozott anyagi kár azonban a környező időszak összes kárát tekintve elenyésző volt. (Nem érte el az 50 milliárd dollárt!) A károk tekintetében rekordnak a 1995-ös és a 2005-ös év tekinthető több mint 200, illetve 150 milliárd dollárral.

A fenti grafikonokat párhuzamba állítva és összefüggéseiben elemezve számos fontos következtetést vonhatunk le:

- A katasztrófák száma, valamint az érintettek, áldozatok száma és az anyagi károk között nem határozható meg „ököl szabály-szerű” összefüggés.

- Az érintettek és áldozatok száma, valamint anyagi károk tekintetében alapvető fontossággal bír a „földrajzi tényező”:
- A magasan fejlett, sűrűn lakott területeken bekövetkező események sok embert érintenek, jelentős károkat okoznak, ugyanakkor általában „kevés” halálos áldozatot követelnek. (Az 1995-ben Japánban, Kóbé-ban bekövetkező földrengés csak egy volt az év közel 450 katasztrófája közül, mégis a maga 121 milliárd dolláros kártételével az összes kár közel 60%-át tette ki. Még szembetűnőbb a helyzet a 2005-ben, az USA-ban tomboló Katrina és Rita hurrikánok esetében, amikor is a közel 800 katasztrófa által együttesen okozott közel 160 milliárd dolláros kárból több mint 131 milliárd keletkezett az általuk sújtott területeken (~81%!).
- Alacsonyan fejlett sűrűn lakott területeken bekövetkező események sok embert érintenek, „kisebb” károkat okoznak, jelentős számú halálos áldozatot követelnek. (Ezek a megállapítások gyakran ritkábban lakott területek esetén is érvényesek!) (Példaként említhetnénk az Indiai, Pakisztáni, és Iráni városokat sújtó földrengéseket, illetve a 2004 karácsonyán a délkelet ázsiai térséget súlytó szökőárat.)
- Az Európában egyre gyakrabban bekövetkező hidro-meteorológiai katasztrófák (pl. 2000, 2002) az évszázados tapasztalatoknak, a kiépített védműrendszereknek, a katasztrófavédelem magasan fejlett szervezetének, irányítási- és vezetési rendszerének köszönhetően még magas eseményszám és óriási érintett népesség mellett is viszonylag kevés halálos áldozatot követelnek, és a korábban említettekhez képest szinte elenyésző anyagi természetű kárt okoznak.
- A civilizációs katasztrófák (ide értve a terrortámadásokat is) a természeti pusztításokhoz képest elenyésző számú népességet érintenek közvetlenül, „kevés” halálos áldozatot és anyagi kárt eredményeznek. A terrorcselekmények következtében kialakuló veszélyhelyzetek pszichológiai hatása (mind az érintett lakosságot, mind pedig a Föld teljes népességét tekintve) azonban sokkal jelentősebb, mint egy hasonló mértékű természeti katasztrófé. (Bár 2001. szeptember 11-én összeomlott a Világkereskedelmi Központ két tornya, abban az évben az okozott károkat leíró függvénynek lokális minimuma volt. Ugyanakkor - az okozott globális sokkhatásnak köszönhetően - a világgazdaságban bekövetkező visszaesés által okozott közvetett kár talán csak tízezer milliárd dollárokban és hosszú években mérhető!)

A fenti tendenciákat és következtetéseket figyelembe véve megállapítható, hogy mind a természeti, mind pedig a civilizációs veszélyhelyzetek évről évre

egyre jelentősebb fenyegetést jelentenek az emberiségre. A cikk írásakor⁸⁰ Magyarország túl van a valaha látott legjelentősebb árvízén, Budapest az elmúlt évtizedek legpusztítóbb viharán, Indonézia egy újabb szökőáron, Kínában milliókat telepítettek ki az óriási áradások miatt, erdőtüzek tombolnak Spanyolországban, Portugáliában, Görögországban, Törökországban és a Föld számos országában, Európa túl van az elmúlt évszázad egyik legjelentősebb hőhullámán, míg Nagy-Britanniában, az Egyesült Államokban, Németországban és számos államban terrorriadók követik egymást...

Ezen (koránt sem teljes) felsorolás is nyomatékot ad a katasztrófavédelem egyre növekvő szerepének, jelentőségének. A katasztrófavédelem, mint bonyolult és komplex rendszer, a világ minden pontján (így Magyarországon is) számos hatóság, szervezet (politikai és szakmai irányító szervek, a Katasztrófavédelem, Polgári védelem, Tűzoltóság, Rendőrség, Honvédség, Határőrség, Mentőszolgálat, valamint számos más helyi és országos hatáskörű szervezet), állami és polgári vállalat, valamint a lakosság együttműködését igényli a hatékony védekezés végrehajtása érdekében. Ennek megvalósításában kiemelt szerep jut az információk cseréjének, a kommunikációnak. A legfontosabb feladatok egyike, hogy a mentésben, illetve védekezésben résztvevők állandó összeköttetésben legyenek egymással, a technikai eszközök kezelőivel, a munkálatokat irányító helyi és központi parancsnokságokkal.

Az ilyen hírközlési rendszerek esetében alapvető követelmény a folyamatos rendelkezésre állás, valamint a biztonságos együttműködési képesség (kompatibilitás). Érdemes tehát számba venni azon elektronikus hírközlési rendszereket, melyek szóba jöhetnek egy katasztrófa esetén a védekezés kommunikációs támogatásának biztosításában.

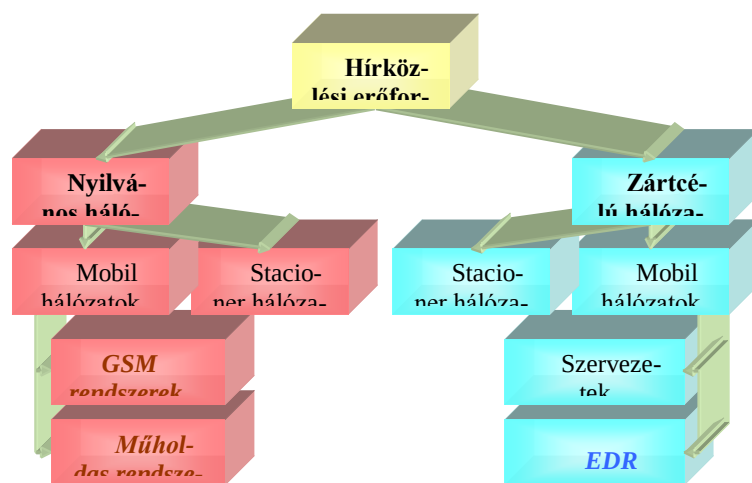
Hírközlő rendszerek a katasztrófavédelemben⁸¹

A védekezés előkészítése és lebonyolítása során a „forgalmazás” jelentős hányada – a jelenlegi állapotok szerint⁸² – a különböző szervezetek zártcélú hálózataival mellett a vezetékes, és elsősorban a mobiltelefon szolgáltatók hálózataival bonyolódik. A rendelkezésre álló hálózattípusokat rendeltetés szerint csoportosítva az 5. ábra mutatja.

⁸⁰ 2006. augusztus

⁸¹ Cikkemben kizárólag az 'alárendeltek' vezetését és a köztük történő információcserét (a védekezés során) biztosító, mobil kommunikációt lehetővé tevő rádiófrekvenciás rendszerekkel kívánok foglalkozni.

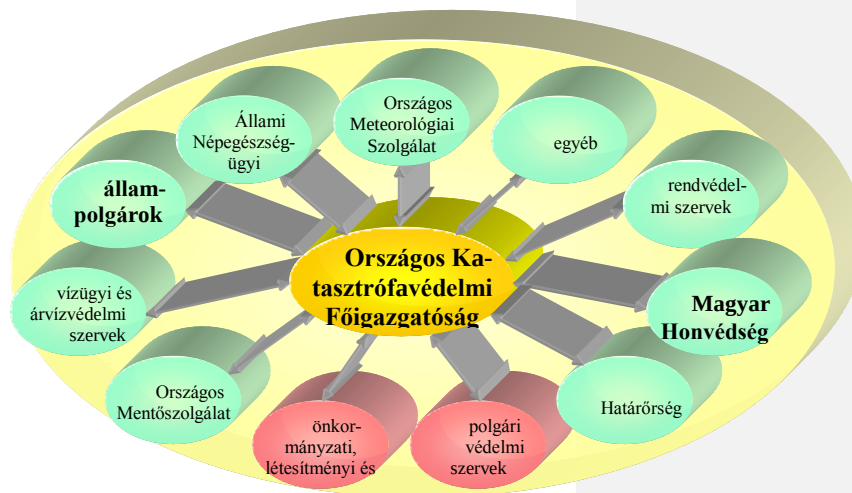
⁸² 2006. augusztus



4. ábra: Az igénybe vehető hírközlő rendszerek (Forrás: szerző)

A fenti ábrán megjelenő erőforrás csoportok kifejtését érdemes - a mai helyzetet kiindulási alapnak tekintve - a katasztrófavédelem rendszerében valamilyen szerepet betöltő szervezetek zártcélú rádiórendszereinek kompatibilitási kérdésével kezdeni, hogy megértsük a megoldásra váró kommunikációs anomáliák hátterét.

A katasztrófavédelmi tevékenységek tervezésével, szervezésével, irányításával, és koordinálásával az Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: OKF) foglalkozik, így mint központi szerv áll a kapcsolati rendszer központjában. Az OKF együttműködőkkel fennálló fontosabb kapcsolatait a 6. ábra szemlélteti.



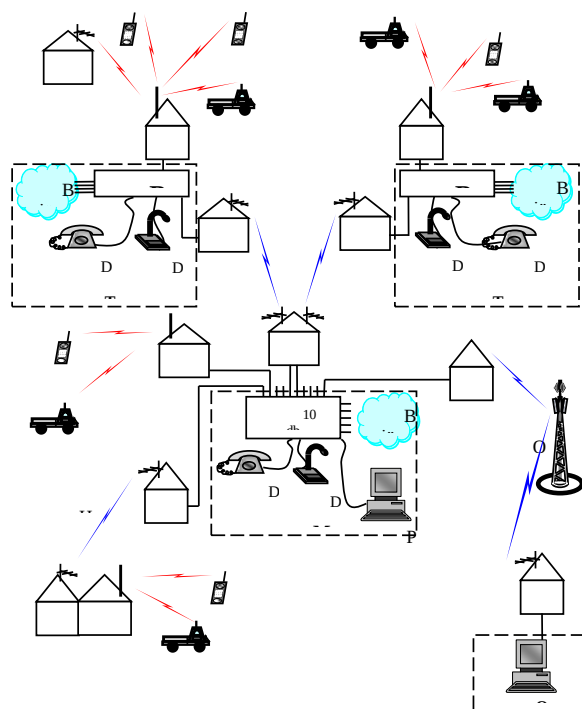
5. ábra: Az OKF és együttműködők kapcsolatai (Forrás: szerző)

Az OKF bonyolult és sokrétű feladatrendszeréből adódóan több rádiókommunikációs rendszert is üzemeltet, amelyek funkcióikat tekintve két nagy csoportba sorolhatók. Egyik csoportba az információs, segélyhívó, viharjelző, riasztó, és tájékoztató rendszerek⁸³, míg másikkba a katasztrófavédelmi URH és RH rádiórendszerek tartoznak. A rádióhíradás rendszertechnikai szerkezetére a hármas tagozódású centralizált felépítés jellemző. A piramisszerű, hierarchikus rendszer alapján, a települések vonzáskörzetében jelentkezik a hírközlési igény jelentős hányada, ami a vezetési szinteken feljebb haladva egyre csökken. Ezt a struktúrát követve alakították ki a rendszer jogosultsági szintjeit és átbocsátóképességét, így a struktúrába felfelé haladva a hírközlési keresztmetszet csökken, míg az igénybe vehető szolgáltatások száma és színvonala nő. Az országos rendszer vázlatos felépítését a 8. ábra szemlélteti.

A települési hírrendszerek városi átjátszói tartalmaznak egy 300MHz-es bekötő állomást és egy BGY-9000-es átjátszó vezérlő automatikát, amely négy csatlakozási lehetőséget biztosít az együttműködő szervezetek (pl. HM, BM) vonalainak illesztésére. A rádióállomások önállóan is képesek távvezérléssel ezen vonalak elérésére, míg a bejövő hívások kapcsolása digitális telefonközpont esetén automatikusan, egyéb esetekben diszpécser, vagy egy kijelölt alállomás segítségével történik. Ez a megoldás lehetőséget biztosít, hogy katasztrófavédelemben, a védekezésben résztvevő szervezetek hírrendszereit

⁸³ Dunai Információs Segélyhívó Rendszer (DISR), Tiszai Információs Segélyhívó Rendszer (TISR), Balatoni és Velencei-tavi Viharjelző Rendszer, Lakossági riasztó és tájékoztató rendszerek

(ha csak szűk keresztmetszeten is) helyi szinten illeszteni lehessen az OKF hálózatához. Ez a lehetőség megyei szinten is rendelkezésre áll (max. 5 telefonvonal).



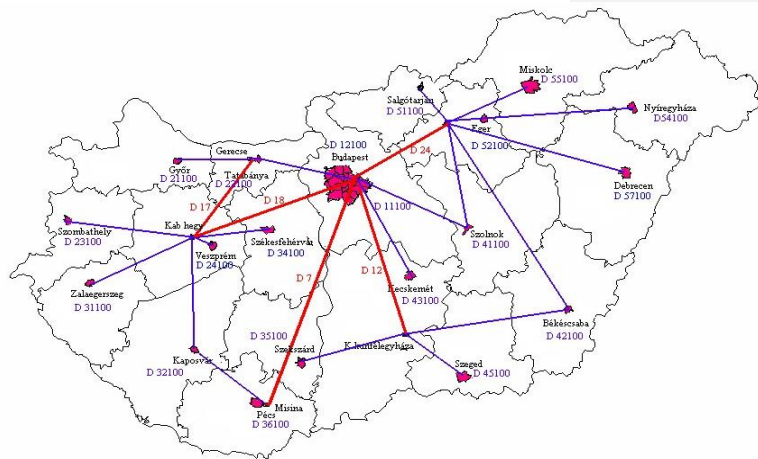
8. ábra: OKF országos rádiórendszere (Forrás: szerző)

A megyei hírendszerek feladata adott esetben a települési hálózatok forgalmának menedzselése, összekapcsolásának biztosítása, továbbá átviteli út megvalósítása egyes megyei átjátszók és az országos rendszer felé. A megyei rendszerek az ügyeleteken elhelyezett központokra, az ide bekötött átjátszókra, és az országos bekötőre épülnek. A központ egy digitális vezérlésű BGY-9500 (10 rádiócsatornás) automatikát tartalmaz, ami lehetővé teszi a hozzá illesztett rádióháló összekapcsolását, valamint „trónkölését”. A megyei és városi átjátszók száma a terepviszonyok függvényében úgy változik, hogy biztosítsa a teljes lefedettséget. A központok nyilvántartják a körzetükben tartózkodó alállomásokat. Ha számukra addig ’idegen’ állomás jelentkezik be, jelentik azt az „anyaközpontnak”, valamint ha saját készülékeik körzethatárt lépnek át,

elvégez a hívásátírányításokat, illetve egy adatbázis segítségével naplózzák a forgalmat.

Az országos rendszer (gerinchálózat) rendeltetése összeköttetést biztosítani az egyes megyei központok között, valamint az országos hatáskörű együttműködő szervezetek hálózatai felé. Felépítése a megyei központokéhoz hasonló. Egy budapesti számítógépes központból, valamint a 300 MHz-en bekötött országos átvírószókból áll. A központ nyilvántartja a megyék elérhetőségi irányait, és továbbítja azok jelzéseit.

A megyék központjai a számukra kijelölt öt rádiófelvevő pont (átvívószók: Kékestető, Kabhegy, Misina, Kiskunfélegyháza, Gerecse) valamelyikén keresztül csatlakoznak a budapesti központi átvírószóhoz. (9. ábra)



9. ábra: Az OKF URH rendszerének átvírószói és irányai (Forrás: OKF)

A fent ismertetett rendszer a polgári védelmi feladatok híradásának biztosítását közel 40 rádiócsatornával képes rugalmasan (adott feladatra optimalizálva) ellátni az ország egész területén, ezzel az ország egyik legkorszerűbb rádiórendszerének számít. Bizonyos mértékig, ha szűk keresztmetszetben is képes összeköttetést biztosítani az együttműködő szervezetek hírszerei felé, ugyanakkor egyáltalán nem kompatibilis az országban használt egyéb készenléti rádiórendszerekkel.

Nincs ez másként a tűzoltóságok által alkalmazott 150 MHz-es szimples csatornákat biztosító rendszer esetében sem, amely azonban nem nyújt az előzőhöz hasonló országos lefedettséget. Ez a rendszer tulajdonképpen nem

más, mint egymástól független megyei szintű szimplex rádióhálóok összessége, közel 3000 tagállomással.

A rendőrség saját szervezetén belül is számos, egymással sem kompatibilis rendszer üzemel (szimplex, félduplex, duplex), így gyakran két szomszédos kerület egységei sem tudnak egymással összeköttetést létesíteni.

A mentők egységes Motorola rendszert használnak, míg a büntetés végrehajtás híradásának biztosítására a rendőrségi rendszereket használják (szimplex).

A határőrség rádióhíradását kétféle rádiórendszer (MOTOROLA, TMRK) a határ mentén telepített 76 db bázisállomással biztosítja, amely viszonylag korszerű technológiai színvonalának és nyújtott szolgáltatásainak köszönhetően a határok térségében kielégíti a szervezet vezeték nélküli hírközlési igényeit, azonban az új feladatrendszerben megjelenő mélységi feladatok kommunikációs támogatását nem képes ellátni.

A Magyar Honvédség tábori híradását biztosító rádiórendszerek természetesen teljesen függetlenek a fenti szervezetekétől, de alapvető rendeltetésüket tekintve nem is követelmény az ezekkel való interoperabilitás.

Összességében megállapítható, hogy a készenléti szervezetek vezeték nélküli kommunikációs csatornáit biztosító rendszerek a kompatibilitás (együttműködő képesség) legalapvetőbb követelményeinek sem felelnek meg. Bár az OKF (PVOP) vezeték nélküli hálózata alkalmas helyi-, együttműködési-, valamint országos szintű rádióhíradás megszervezésére, több megyét, vagy az ország területének jelentős részét érintő nagyobb kiterjedésű katasztrófa esetén a rendelkezésre álló szűk keresztmetszet következtében („kárhelyszín együttműködési csatorna” 152,7 MHz), még a beiktatott prioritások mellett sem képes a forgalom zökkenőmentes lekezelésére. (Torlódások!) Az alapvető megoldást természetesen egy országos készenléti rádiórendszer kiépítése jelenti, amelyben biztosítható az alkalmazó szervezetek belső híradása, valamint katasztrófahelyzetben azok összekapcsolásával az együttműködési híradás...

Egységes Digitális Rádiótávközlő Rendszer (EDR)

A fent említett kompatibilitási anomália feloldására - több mint egy évtizedes halogatás után – 2003-ban döntés született⁸⁴, így lehetővé vált a készenléti és kormányzati felhasználói kör rádiókommunikációs igényeinek kielégítésére alkalmas, a Schengeni egyezmény követelményeinek és az ETSI⁸⁵ szabványainak megfelelő digitális rádiótávközlő rendszer megvalósításának előkészítése. A kivitelezésre vonatkozó nyílt, kétfordulós, tárgyalásos közbeszerzési eljárás előkészítését és lefolytatását követően, a Miniszterelnöki Hivatal EDR Kormánybiztosa a győztes T-Mobile Magyarország Rt. - Magyar

⁸⁴ 1031/2003. (IV. 09.) kormányhatározat

⁸⁵ Európai Távközlési Szabványosítási Intézet

Telecom konzorciummal 2005 végén megkötötte a szerződést. A szerződés alapján a konzorcium saját erőforrásból (a felhasználható állami vagyonelemeket, erőforrásokat és ellentételezési lehetőségeket a lehető legteljesebb módon hasznosítva) biztosítja az országos hálózat kiépítését, üzembe helyezését, üzemeltetését és üzemben tartását, valamint az így létrejövő infrastruktúrán anyagi ellentételezés fejében szolgáltatásokat biztosít a rendszer igénybevételeire kötelezett készenléti és kormányzati szervezetek számára. (Vagyis a Rendőrség; Határőrség; Tűzoltóság; Katasztrófavédelem; Országos Környezetvédelmi, Természetvédelmi és Vízügyi Főigazgatóság; Büntetésvégrehajtás; Nemzetbiztonsági Szolgálatok; Országos Mentőszolgálat; Magyar Honvédség; Vám- és Pénzügyőrség stb. bérlő a rádióhíradását egy polgári szolgáltatótól, így a rendszer tulajdonképpen egy negyedik, speciális mobiltelefon hálózatként is aposztrofálható!)

Az országos hálózat kiépítésének első fázisaként 2006. április 5.-ére elkészült és megkezdte próbaüzemét a 39 bázisállomásból és két átjátszóállomásból álló Budapesti rendszer, amely szolgáltatásainak igénybevétele a készenléti szolgálatok mintegy 14 000 végberendezést bérelnek. A teljes magyarországi rendszer (200-300 bázisállomás) várhatóan 2007. január 31.-éig kerül átadásra, így az ország területének mintegy 94%-án válik lehetővé további 28 000 felhasználó számára a szolgáltatások széles körének igénybevétele, 99,9%-os rendelkezésre állás mellett.

Az EDR a TETRA⁸⁶ technológiára épül, mely egy, a professzionális felhasználói igények kielégítésére alkalmas mobil hírközlő rendszer szelektív- és csoportkommunikációs beszéd és adatátviteli szolgáltatásokkal. Alkalmazhatóságát a fejlett digitális jelfeldolgozási eljárásokra épülő átviteltechnika által biztosított zavarcsökkentett összeköttetések létesítésének lehetősége, a magas rendelkezésre állás, a gyors hívásfelépítés (~0,5s), információvédelmi megoldások, és számos egyéb járulékos szolgáltatás biztosítja.

A TETRA rendszer által nyújtott szolgáltatások - más hírközlő rendszerhez hasonlóan - három csoportba sorolhatók. A *teleszolgáltatások* a végfelhasználói rádióterminál segítségével vehetők igénybe (pl. beszédhívás), míg a *hordozószolgáltatások* eléréséhez valamilyen külső berendezés csatlakoztatására van szükség (pl. számítógép, GPS vevő). A *kiegészítő szolgáltatások* a teleszolgáltatásokat (vagy azok igénybevételeének módját) változtatják meg, illetve egészítik ki.

Az egyéni⁸⁷-, csoport-, körözvény- és expressz⁸⁸ hívás a fentiek alapján a teleszolgáltatások csoportjába tartozik. A *csoporthívás*, mint a készenléti szervek beszédkommunikációjának legfontosabb platformja, – a katonai al-

⁸⁶ Trans-European Trunked Radio

⁸⁷ One - to - one

⁸⁸ Push and talk

kalmazásoknál megszokott rádióháló szervezésű híradáshoz hasonlóan - egy félduplex megoldás. Ez annyit jelent, hogy egy csoportban egyidejűleg csak egyetlen tagállomás forgalmazhat, míg a továbbított információt a többi felhasználó hallgatja. A teljes TETRA hálózaton egyszerre akár több száz, egymástól teljesen független beszédcsoport is üzemelhet egymás zavarása nélkül, ami biztosítja a rendszert használó készenléti szervezetek és más felhasználói csoportok biztonságos híradását. Egy terminálra feltöltött beszédcsoportok közül a kezelő a csoportválasztó gomb (vagy menü) segítségével tudja kiválasztani a számára aktuálisan éppen szükségeset. A hálózatba definiált, megfelelő jogosultságokkal rendelkező diszpécser képes nagyon rövid idő alatt az egyes csoportok összekapcsolására (közös beszédcsoportba történő rendezésére), ami nagyban segíti - például egy katasztrófa esetén - a mentésben résztvevő különböző egységek (rendőrök, mentők, katonák stb.) közti együttműködést. (Ez a megoldás - az egységes európai szabványnak köszönhetően - nemzetközi feladatok együttműködési híradásának szervezésére is alkalmazható!) A felhasználó *egyéni hívásokat* - a hálózatban számára beállított jogosultságoknak megfelelően - kezdeményezhet (és fogadhat) akár saját csoporton belül, akár másik csoportba (TETRA), de lehetséges összeköttetés létrehozása egy másik alközponti szám, illetve nyilvános vezetékes-, vagy mobiltelefon előfizetői szám irányába is. Ebben az esetben a kommunikáció két felhasználó között zajlik, azt más tagállomás nem hallja. A tárcsázás megkönnyítését a beépített telefonkönyv mellett programozott gyorshívó gombok is segíthetik.

A kiegészítő szolgáltatások⁸⁹ számos olyan lehetőséget is biztosítanak a nyilvános hírközlő rendszerek esetében megszokottak mellett (mint például: hívásátirányítás, hívásvárakoztatás, hívástartás, hívástiltás, hívó fél azonosítás), melyek speciálisan a készenléti szervek igényeinek megfelelően kerültek kialakításra. A *vészhívás* funkció a bajba jutott felhasználó számára egyetlen gombnyomással elérhető, melynek következtében segélykérését a csoport összes tagállomása és a diszpécser is fogadja, akár a meglévő összeköttetések bontása árán is. A *dinamikus csoport hozzárendelés*⁹⁰ segítségével lehetőség van arra, hogy a jogosultsággal rendelkező diszpécser a hálózaton keresztül, a technikailag arra alkalmas terminálokra újabb csoportokat programozzon, vagy adott feladat végrehajtása érdekében független csoportokban tevékenykedő felhasználókat közös csoportba szervezzon. (A feladat végrehajtását követően a feltöltött csoportokat a diszpécser törölheti.) A *belehallgatás*⁹¹ funkció segítségével, a jogosultsággal rendelkező diszpécser betekintést nyerhet a saját felügyelete alá tartozó két felhasználó közti hívásba (azok tudomása nélkül), ezzel ellenőrizve például a forgalmazás szabályainak betartását. Hasonló

⁸⁹ Cikkemben kizárólag a készenléti szervek szempontjából jelentős szolgáltatásokkal kívánok foglalkozni

⁹⁰ DGNA (Dynamic Group Number Assignment)

⁹¹ DL (Discreet Listening)

szolgáltatás a *környezet figyelés*⁹², melynek aktiválása esetén a jogosult diszpécser (parancsnok) a saját csoportjában bármely rádióterminált észrevétlenül adásra kapcsolhatja, így szereztve tudomást például egy ipari baleset, vagy a valamilyen okból kifolyólag tevékenységében korlátozott felhasználó környezetében történetekről.

Mind az áramkör-, mind pedig a csomagkapcsolt adatátvitellel, illetve a rövid adatokkal kapcsolatos szolgáltatások a hordozószolgáltatások csoportjába tartoznak. TETRA hálózatokon hibajavító képesség szempontjából háromféle *áramkörkapcsolt adatátvitel* valósítható meg, mint a különösen védett 2,4 kbit/s, a védett 4,8 kbit/s és védelem nélküli 7,2 kbit/s sebességű. Ilyen jellegű összeköttetések esetén az átviteli csatorna a hívás idejére, forgalomtól függetlenül lefoglalásra kerül, mely a hálózat áteresztőképességének szempontjából nem túl előnyös, ezért ezt a megoldást ritkán használják. A *csomagkapcsolt adatátvitel* rugalmasságának köszönhetően sokkal elterjedtebb megoldás, hiszen ebben az esetben a hívás ideje alatt ugyan folyamatos összeköttetés jön létre a logikai csatornán, a fizikai csatorna (7,2 kbit/s) azonban csak a tényleges forgalom függvényében kerül lefoglalásra. (A hibajavításról ebben az esetben az igénybevett alkalmazásnak kell gondoskodnia.) A *rövid adat*⁹³ szolgáltatás négyféle hosszúságú üzenet (16, 32, 64, 2047 bit) továbbítására biztosít lehetőséget, melyek segítségével státuszüzenetek, GPS⁹⁴ adatok és SMS⁹⁵ üzenetek küldhetők.

A fenti szolgáltatások biztosításához szükséges rendszerinfrastruktúra gyártónként változhat, hiszen a TETRA szabvány nem definiál egyetlen hálózati elemet, vagy interfészt sem. A rendszernek azonban mindenképpen tartalmaznia kell bázisállomás adó-vevőket a rádió interfész biztosítására, kapcsolóközpontokat a hívások felépítésére és kezelésére, adatbázisokat a felhasználók azonosítására, hálózat-felügyeleti központot a rendszer működésének irányítására, ellenőrzésére, valamint kapukat más hírközlő hálózatokhoz való csatlakozás biztosítására. A 10. ábrán a Nokia TETRA rendszerének általános felépítése (egy változat) látható (Magyarországon is ez a rendszer épül ki!), mely rugalmasan alakítható struktúrával, cellás mobiltelefon hálózatként képes a felhasználó szervezetek saját és együttműködési kommunikációs igényeinek kielégítésére.

A rendszer elemei ennek megfelelően a különböző topológiába szervezhető, rugalmasan bővíthető, távkonfigurálható bázisállomások (TBS⁹⁶),

⁹² AL (Ambience Listening)

⁹³ SDS (Short Data Service)

⁹⁴ Global Positioning System (Globális Helymeghatározó Rendszer)

⁹⁵ Short Message Service (Rövid Szöveges Üzenet Szolgáltatás)

⁹⁶ TETRA Base Station

melyek teljes kiépítésben⁹⁷ egyenként legfeljebb 32 fizikai csatornát képesek kiszolgálni (ebből egy vezérlőcsatorna), amivel akár nagy forgalmú területek is elláthatók. A nagytartalékolású, hibatűrő, nagykapacitású kapcsolóközpontok (DXT⁹⁸) – melyek jelentős számú interfészt biztosítanak a bázisállomások, diszpécserközpontok, más központok, alközponti rendszerek, rádiórendszerek, valamint más analóg és digitális hírközlő rendszerek felé – tartalmazzák a felhasználók azonosításához szükséges adatbázisokat (HLR⁹⁹, VLR¹⁰⁰). Hierarchikus központhálózatok esetén keletkező átmenő forgalmat olyan DXT tranzitközpontok (DXTT) kezelik, melyek nem alkalmasak ugyan bázisállomások kiszolgálására, átbocsátóképességük azonban jelentősen meghaladja az „egyszerű” DXT központokét. A különböző informatikai hálózatok az IP gerinchálózaton csatlakozó GGSN¹⁰¹ átjárón keresztül illeszthetők a TETRA rendszerhez.

A diszpécserrendszerek (DWS¹⁰²) alapvető feladata a hozzájuk tartozó szervezet (pl. rendőrség, mentők, honvédség) virtuális magánhálózatának (hálózatainak) menedzselése, azaz a felhasználók tevékenységének figyelése, követése, a jogosultságok és szolgáltatások definiálása, felhasználói csoportok összerendelése stb.

A teljes hálózat üzemeltetését biztosító NetAct hálózatfelügyeleti rendszer végzi a hibák kezelését, a hálózati elemek konfigurálását, működési adatok gyűjtését, tárolását, feldolgozását. A magyarországi TETRA rendszer tehát a fentiek alapján, végleges üzembe helyezését követően, alkalmassá válik a készenléti szervek és más szervezetek vezeték nélküli hírközlési igényeinek kielégítése úgy normál körülmények között, mint katasztrófavédelemmel összefüggő tevékenységek, valamint belföldi és nemzetközi együttműködést igénylő feladatok végrehajtása esetén. Ezt a világ számos országában működő - különböző rendeltetésű - közel 700 TETRA hálózat alkalmazási tapasztalatai is bizonyítják.

Nyilvános mobiltelefon hálózatok alkalmazásának lehetőségei

Az 1053/2005. kormányrendelet értelmében, a TETRA rendszer országos üzembe helyezését követő három hónapon belül, a hálózat szolgáltatásainak igénybevételére kötelezett állami szervezeteknek a más módon nem hasznosítható saját rádióhírközlő rendszereit fel kell számolniuk, és ezt követően vezeték nélküli forgalmazásra az EDR-t kell igénybe venniük¹⁰³.

⁹⁷ Bővítő szekrénnel 8 TETRA adó-vevő (TTRX - TETRA Transmitter-Receiver), adó-vevőnként 4 csatorna

⁹⁸ Digital Exchange for TETRA

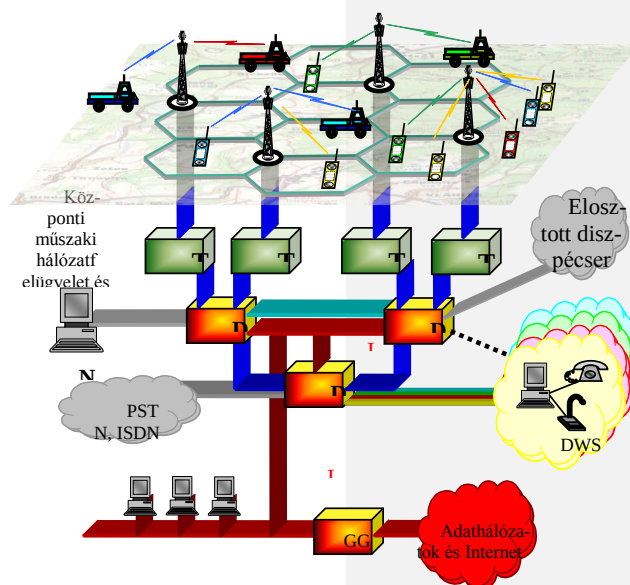
⁹⁹ Home Location Register (Honos Helyzetregiszter)

¹⁰⁰ Visitor Location Register (Látogató Helyzetregiszter)

¹⁰¹ Gateway GPRS Support Node

¹⁰² Dispatcher Workstation

¹⁰³ Ez alól csak a Magyar Honvédség tábori hírendszere a kivétel.



10. ábra: A Nokia TETRA rendszerének felépítése (egy változat) (Forrás: a szerző)

Mi történik azonban akkor, ha valamilyen természeti katasztrófa, szándékos rongálás, terrortámadás következtében, vagy más okból kifolyólag (pl. energiaellátás kiesése, szoftverhiba) üzemzavar lép fel, illetve a hálózat használhatatlanná válik. Ilyen esetekben is mind normál üzemvitel, mind pedig katasztrófhelyzetben biztosítani kell a zavartalan információtovábbítás lehetőségét. Egyéb párhuzamos (redundáns) rendszerek hiányában legkézenfekvőbb megoldásnak a nyilvános mobiltelefon hálózatok igénybevétele tűnik, hiszen mind az infrastruktúra, mind pedig a nyújtott szolgáltatások tekintetében mutatkozik átfedés a két rendszer között. **(GSM, mint véstartalék!)**

A polgári célú mobiltelefon rendszerek ezen felül rendelkeznek azzal az előnnyel, hogy a piac igényeihez igazodva (szabad piaci verseny), a folyamatos fejlesztések következtében, gyorsan nő hálózati infrastruktúrájuk, és az abban alkalmazható felhasználói végberendezések (mobiltelefonok, kommunikátorok) technikai és technológiai színvonala, és ezáltal az igénybe vehető szolgáltatások száma és minősége. Számos olyan szolgáltatást is biztosítanak, melyek a TETRA rendszerben (elsősorban a szűk adatátviteli keresztmetszet, és az alapvető rendeltetésből eredő „hiányosságok” miatt) nem elérhetőek,

mint például az MMS¹⁰⁴, szélessávú adatátvitel, valós idejű videó kommunikáció. **(GSM/UMTS, mint kiegészítő/hiánypótló megoldás!)**

A GSM rendszerek alkalmazása speciális helyzetekben azonban nem csak futurisztikus ábránd, hiszen úgy Magyarországon, mint az egész világon több ízben bizonyította létjogosultságát. Hazai viszonylatban az első „kampányszerű” bevetése a mobiltelefonoknak a 2000-ben a nagy tavaszi tiszai árvíznél volt, amikor is a védekezési területeken nem volt jelentős a mobil hálózati ellátottság, a rendelkezésre álló egyéb rádióhírközlő rendszerek pedig nem voltak képesek biztosítani a hatékony vezetés, irányítás és együttműködés feltételeit a munkálatokban résztvevő tucatnyi szervezet és több mint tízezer ember számára. A szolgáltatók¹⁰⁵ a helyzet normalizálása érdekében számos ideiglenes és mobil (mozgatható) bázisállomást telepítettek, és több száz készüléket osztottak szét a munkálatokban résztvevő szervezetek között, amivel sikerült az érintett területek „híradását” megnyugtatóan rendezni. Az azóta eltelt hat évben a veszélyhelyzeti hírközlést szervező és tervező szakemberek már kiemelt szerepet szántak a hasonló jellegű megoldásoknak. A 2002-es és 2006-os árvizek idején, a védekezési munkálatokat a helyszínen irányítók saját készülékeik (szolgálati és/vagy privát) telefonkönyvében tárolták közvetlen beosztottaik, valamint az együttműködő szervezetek munkacsoportjait vezető személyek hívószámait, és ezek segítségével hangolták össze a védekezésben résztvevők munkáját.

A mobiltelefonok azonban nem csak a védekezésben résztvevők kommunikációs igényeinek kielégítésére alkalmasak. 2006. júniusában Magyarországon a 9 447 206 hívásfogadásra alkalmas SIM kártya közül 8 806 761 az elmúlt három hónapban forgalmat is bonyolított, azaz a 100 lakosra jutó előfizetések száma 93,7 volt¹⁰⁶. Ez azért fontos adat, mert kiderül belőle, hogy a teljes népesség túlnyomó többsége elérhető mobiltelefonon, ami lehetőséget biztosít a katasztrófák által fenyegetett, illetve sújtott területeken élők veszélyhelyzeti tájékoztatására. **(Mobiltelefon, mint a lakossági tájékoztatási rendszer része!)** A fent említett funkció alkalmazására a legfrissebb és legjobb példa a 2006. júliusában Izrael által Libanon ellen indított offenzíva, melynek gerincét a légítámadások adták. Az érintett területek lakosait a libanoni hatóságok SMS-ben tájékoztatták várható csapás helyéről, idejéről és a menekülési útvonalakról (helyfüggő szolgáltatás). Ezen megoldás alkalmazásával valószínűleg több száz emberéletet mentettek meg... Hazai viszonylatokra is adaptálható ez a riasztási rendszer például nukleáris (Paks), ipari és vegyi balesetek, vagy akár az árvízi kitelepítések során.

¹⁰⁴ Multimedia Message Service – multimédiás üzenetküldési szolgáltatás

¹⁰⁵ A Westel (most T-Mobile) és Pannon GSM is saját költségvetéséből finanszírozta az „akciót”.

¹⁰⁶ Forrás: NHH (Nemzeti Hírközlési Hatóság) Mobil Gyorsjelentés

A fent említettek ellenére azonban a mobiltelefonok legkézenfekvőbb, és a mai napig is leggyakrabban igénybevett veszélyhelyzeti alkalmazása a segélykérés (112), melyet a mobiltelefon hálózatok kiemelt prioritással kezelnek. Ez annyit jelent, hogy a vészhívások a rendszer teljes leterheltsége esetén, akár fennálló összeköttetések megszakítása árán is létrejönnek. **(Mobiltelefon, mint a segélykérés eszköze!)**

Az „egyszerű” segítségkérés mellett azonban a jelenlegi rendszerek technikailag és technológiailag is alkalmasak adott végberendezés helyzetének GSM estén 50m-es, UMTS esetén 10m-es pontossággal történő meghatározására. Ez segélyhívás esetén számos európai országban már automatikusan megtörténik (E112), míg Magyarországon csak speciális esetekben, elsősorban a szervezett bűnözés elleni harc esetén működik. (Szükségesnek tartom az E112, helyadatokkal kiegészített segélyhívó rendszer hazánkban történő mielőbbi bevezetését!) Az 50 illetve 10 m-es pontosság megfelelő lehet ritkán lakott területeken történő helymeghatározásra, azonban nagyvárosokban, vagy tömegrendezvények helyszínein ez nem minden esetben nyújt elegendő bizonyosságot. Számos technológia mellett, az adaptív antennarendszerek fent említett területek ellátását biztosító bázisállomásain történő alkalmazása jelentősen növelheti a helymeghatározás pontosságát. (Akár cm-es pontosság is elérhető!) **(Mobiltelefon hálózat, mint a helymeghatározás eszköze!)**

A fentiek figyelembe vételével vizsgáljuk meg, milyen módszerekkel, technikai megoldásokkal és milyen szolgáltatások igénybevételével lehet a mobiltelefon szolgáltatók hálózatainak képességeit hatékonyabban felhasználni a veszélyhelyzeti hírközlés igényeinek kielégítésére, biztonságának növelésére.

Katasztrófa helyzetben jelen pillanatban is a mobiltelefon jelenti a mozgósítás leghatékonyabb, a kapcsolattartás legmegbízhatóbb lehetőségét a Rendőrség, Mentőszolgálat, Katasztrófavédelem, Honvédség és más, a krízis felszámolásában résztvevő szolgálat vezetői, szakemberei és beosztott állománya számára. A mobiltelefon hálózatok jelenlegi technológiai és technikai felépítése és működési elve lehetőséget nyújt arra, hogy krízishelyzetben a kiemelt fontosságú felhasználók számára „**elsőbbségi hozzáférést**” biztosítson. Ehhez egy olyan speciális, többszintű „**hatósági hozzáférés vezérlő rendszert**” (**HHVR**) kell kialakítani, ami szükség esetén lehetővé teszi a GSM (UMTS) hálózatok „**normál üzemi**” működésének gyors átállítását egy „**krízis üzemmódba**”, amely biztosítja a rendszer erőforrásainak rugalmas felhasználását a kialakult helyzet súlyosságának, a mentésben résztvevők kommunikációs igényeinek, illetve a közbiztonság (terrorelhárítás, szervezett bűnözés elleni küzdelem), nemzetbiztonság, vagy nemzetgazdaság érdekeinek megfelelően. Ez a „rendszer átállítás” a kialakult rendkívüli helyzet által érintett területek nagyságától függően korlátozódhat néhány cellára, de kiterjedhet

városrészekre, városokra, sőt országrészekre, vagy akár az ország egész területére. Természetesen egy ilyen megoldás alkalmazása számos megválaszolandó kérdést vet fel, mind az igénybevétel körülményeivel, mind pedig a nyújtott szolgáltatásokkal kapcsolatban.

Elsődleges kérdés, hogy ki és milyen rendkívüli helyzetek kapcsán utasíthatja a piaci alapon működő szolgáltatókat a hozzáférés vezérlés aktiválására. A felelősségi körök kialakításánál figyelembe kell venni, hogy a döntési mechanizmus ne növelje jelentősen az intézkedések fogantatásához szükséges időt. (Például, ha egy robbantásos merényletet követően fennáll annak a veszélye, hogy mobiltelefonos távirányításával újabb pokolgépeket hoznak működésbe, a lehető leggyorsabban el kell rendelni a mobil szolgáltatások érintett területeken történő felfüggesztését.) Ugyanakkor a döntés súlyára való tekintettel, azt a lehető legmagasabb szintű felhatalmazás alapján kell meghozni!

A mobiltelefon hálózatokhoz való elsőbbségi hozzáférés (prioritások híváskezelés) biztosításához a készenléti szervek parancsnoki, szakértői, és végrehajtó állománya számára kiutalásra kerülő felhasználói mobil terminálokat olyan speciális SIM kártyával kell ellátni, melyek a hozzáférés vezérlés aktiválását követően lehetőséget biztosítanak az érintett területen a különböző szolgáltatások igénybevételére a hálózatok túlterheltsége, részleges üzemképtenség csökkenése esetén is. A SIM kártyákat úgy kell programozni, hogy mindhárom országos mobil szolgáltató hálózatához hozzáférést biztosítsanak, ezáltal jelentősen növelve az összeköttetések felépülésének valószínűségét, olyan helyzetekben is, ha a kialakult katasztrófahelyzet, vagy terrortámadás, szándékos rongálás következtében valamely rendszer infrastruktúrája nem képes a kívánt szolgáltatások elérését szavatolni. (Normál üzem esetén ezek a speciális terminálok is csak egyszerű mobiltelefonként viselkednek az alapértelmezett hálózatban, és nem biztosítanak prioritást felhasználóik számára.)

Ahhoz hogy megvizsgáljuk, milyen szinteket kell definiálni a HHVR-ben, tisztázni szükséges a mobil kommunikációs rendszereket krízishelyzetben fenyegető jelenséget:

- **Infrastruktúra elvesztése:** amikor egy hálózat valamely része, vagy egésze fizikailag megsemmisül, vagy működésképtelenné válik (pl.: robbantás, földrengés, elemi erejű vihar következtében), illetve az alapvető működéséhez szükséges valamely tényező nem áll rendelkezésre (pl.: energiaellátás zavara, megszűnése; vezérlő szoftverrendszer összeomlása véletlen hiba, vagy szándékos emberi támadás – 'információs terrorizmus' - következtében). Ebben az esetben a rendszer által biztosított szolgáltatások elérhetelenné válnak minden, az adott ellátási területen tartózkodó előfizető számára. (Az összeköttetések megszakadnak)
- **Túlterheltség (vagy túltelítettség):** amikor az igénybevétel nagysága meghaladja a rendszer áteresztőképességét. Ebben az esetben az adott területen

rendelkezésre álló csatornák száma kisebb, mint a híváskezdeményezési próbálkozásoké. (pl.: Újév első percei, vagy bekövetkezett katasztrófát követően)

A gyakorlatban természetesen a két tényező ok-okozati összefüggésben is állhat (például az infrastruktúra egy részének elvesztése a fennmaradó rendszerelemek terheltségének jelentős növekedését okozhatják), illetve egymás hatását erősítve (túlterheltség növekedése újabb erőforrások kiesését okozhatja) akadályozhatja a zavartalan információáramlást.

Következő kérdés tehát, hogy milyen szinteket definiálunk a rendszerben, amihez fel kell mérni azokat az eseményeket, melyek bekövetkeztekor szükségesé válik a HHVR aktiválása. Nézzünk egy alternatívát:

0. szint: a mobiltelefon hálózatok 'normál üzeme': A hálózat forgalma zavartalan, a rendelkezésre álló erőforrások elegendőek, a kezdeményezett összeköttetések létrehozására. A működésbe való beavatkozás nem szükséges.
1. szint: beszédkódolás megváltoztatása (hatósági beavatkozás nélkül a szolgáltató aktiválhatja): Ha valamilyen tömegrendezvény, vagy rendkívüli helyzet (jelentősebb ipari, vagy közlekedési baleset) következtében megnövekedett forgalom túlterheli a hálózatot, akkor GSM rendszer érintett bázisállomásait át lehet állítani teljes sebességű (Full Rate, 13kbit/s) beszédcsatornák alkalmazása helyett félsebességű csatornákra (Half Rate, 6,5kbit/s). Így bár az átvitel minősége és az érthetőség az érintett cellákban romlik, a rendelkezésre álló csatornák száma tulajdonképpen megduplázódik (vivőnként 8-ról 16-ra nő), melynek következtében csökken a rendszer túlterheltsége. (Ezt a megoldást már többször alkalmazták Magyarországon is, például a 2006. tavaszi árvíz idején.)
2. szint: a HHVR aktiválása prioritás biztosításával katasztrófa helyzet esetén: ha egy jelentős mértékű ipari baleset, természeti katasztrófa (2006. augusztus 20-ai elemi erejű vihar), vagy terrortámadás (pl. robbantás) következtében kialakuló túlterheltség a fenti módon már nem kezelhető, akkor a mentésben résztvevő készenléti- és társ-szervek számára a hálózathoz való hozzáférést úgy biztosítják, hogy a speciális SIM kártyával rendelkező mobil készülékekről kezdeményezett hívások prioritást élveznek, akár fennálló összeköttetések bontása árán is. A hívások felépítésének ideje jelentőse csökkenthető, ha az ilyen speciális hívások esetén a szabványos azonosítási eljárást a rendszer mellőzi (vagy jelentősen egyszerűsíti). Mivel a speciális SIM kártya a HHVR aktivitása mellett biztosítja az adott területen elérhető, a védelmi feladatok ellátására kijelölt három országos mobiltelefon szolgáltató hálózataihoz való hozzáférést, lehetőség van arra, hogy hívás kezdeményezésekor a készülék először szabad

csatornákat keressen mindhárom rendszerben, és csak azok hiánya esetén érvényesíti prioritását az alapértelmezett hálózatban. Ha annak sérülése, vagy hibája miatt nem tudja érvényesíteni elsőbbségét, tovább viszi azt a másodlagos, majd harmadlagos hálózatba. Ez a megoldás ugyan növeli a hívásfelépülés idejét, ugyanakkor minimálisra csökkenti az „erőszakos” beavatkozás (kapcsolatbontások) valószínűségét.

3. szint: a HHVR aktiválása, a 'normál' felhasználói forgalom részleges korlátozásával: Amennyiben egy extrém mértékű forgalomnövekedés kezelhetetlen túlterheltséget okoz a szolgáltatók hálózatában (vagy ennek veszélye fennáll), illetve a kialakuló helyzet ezt megkívánja, ennek a szintnek az aktiválásával a 'normál' (prioritással nem rendelkező) előfizetők számára nem engedélyezzük beszélőösszeköttetések létrehozását. Az ilyen készülékekről kizárólag segélyhívás (112) kezdeményezhető, illetve rövid szöveges üzenet küldhető. A prioritással rendelkező felhasználók korlátlanul férhetnek hozzá a hálózathoz.
4. szint: a HHVR aktiválása, a 'normál' felhasználói forgalom teljes korlátozásával: Ez a hatósági hozzáférés vezérlés legmagasabb szintje, amikor is a 'normál' előfizetők kizárólag segélyhívást kezdeményezhetnek. (Ezen szint elrendelésére például olyankor kerülhet sor, ha egy a londonihoz hasonló robbantás sorozatot követően fennáll a veszélye, hogy mobiltelefonos távirányítással újabb pokolgépeket hoznak működésbe.)

A különböző szintek életbeléptetése nem lineárisan, hanem a mindig a kialakult helyzet függvényében történik! Mindegyik szinten lehetőség van mobilizálható (gépjárműbe szerelt) bázisállomások segítségével a rendszer áteresztőképességének növelésére, illetve az esetlegesen kieső erőforrások pótlására.

A HHVR rendszer minden szint esetén biztosítja a segélyhívások lehetőségét minden felhasználó számára, ezáltal nem csorbulhat az állampolgárok biztonságérzete. Ehhez azonban azzal is hozzá kell járulni, hogy azokon a területeken tartózkodókat, amelyeket érint a fenti vezérlési szintek valamelyike, tájékoztatjuk SMS-ben az életbeléptetett korlátozásokról, azok okáról, várható időtartamáról, területi érintettségéről, valamint a korlátozás ideje alatt elérhető szolgáltatásokról. (Ezt közvetlenül az aktiválás előtti időszakban kell megtenni, és így kell eljárni a korlátozások feloldása esetén is!)

Az általam felvázolt HHVR rendszer véleményem szerint rugalmasan képes biztosítani bármilyen típusú katasztrófahelyzetben a készenléti szervek híradását mindaddig, amíg az adott területen bármilyen földi telepítésű mobiltelefon hálózat működőképessége fennáll.

Azt is érdemes megvizsgálni, hogy a mobiltelefon hálózatokon milyen szolgáltatások állnak a katasztrófavédelemben résztvevő szervezetek rendelkezésére.

A rövid szöveges üzenet (SMS) lehetőséget biztosít nagy tömegek egyidejű gyors informálására, amellyel például mozgósítás, vagy lakossági tájékoztatás hatékonyan megoldható. (riasztási és tájékoztatási feladatok)

A GPRS¹⁰⁷ csomagkapcsolt adatátviteli szolgáltatással küldhetünk a GPS¹⁰⁸-szel nyert pontos pozícióadatokat¹⁰⁹, vagy számítógépek között adatfájlokat, dokumentumokat stb. mozgathatunk, vagy hozzáférhetünk központi adatbázisok tartalmaihoz¹¹⁰.

Amennyiben a készülék rendelkezik a szükséges műszaki paraméterekkel, a beépített digitális fényképezőgéppel készített képek MMS¹¹¹-ben azonnal továbbíthatók például az illetékes eljárók, vagy szakértők (pl.: tűzserézszek) felé a gyors helyzetértékelés elősegítése érdekében.

A harmadik generációs hálózatok biztosítják mozgóképek valósidejű továbbítását, ami szintén a katasztrófa következtében kialakult állapot értékelésében segíthet a helyszíntől távoli szakembereknek, továbbá a vezető beosztású személyek részére biztosítja a videokonferencia lehetőségét. Természetesen az UMTS¹¹² technológia szélessávú adatkommunikációs lehetőséget is nyújt a felhasználók számára, ami lehetővé teszi az INTERNET-es tartalmakhoz, vagy a fent említett adatbázisokhoz való gyors hozzáférést.

Gyakran szükség lehet olyan információk titkosított továbbítására, amire a jelenlegi hálózati technológiák nem kínálnak kielégítő megoldást. Léteznek azonban olyan mobiltelefonok (pl. Kongsberg SECTRA NSK 200 Secure Phone¹¹³), amelyek még a szigorú NATO kriptográfiai előírásoknak is megfelelnek, és biztosítják a lehallgathatatlan hang- és adatátvitelt a szabványos mobilhálózatokon.

Végezetül nézzünk egy fiktív példát¹¹⁴ (a Londoni terrortámadás analógiájára):

¹⁰⁷ General Packet Radio Service – csomagkapcsolt adatátviteli protokoll mobil alkalmazásokhoz

¹⁰⁸ Global Positioning System – globális műholdas helymeghatározó rendszer

¹⁰⁹ Akár lakott területeken, akár azoktól távol bekövetkező katasztrófák esetén fontos lehet a mentés mielőbbi megkezdéséhez

¹¹⁰ Személyi adatok terroristák körözéséhez; meteorológiai, geológiai, vízügyi adatok a szükséges felszerelések meghatározásához stb.

¹¹¹ Multimedia Message Service – multimédiás üzenetküldési szolgáltatás

¹¹² Universal Mobile Telecommunications System – univerzális mobil telekommunikációs rendszer

¹¹³ Ilyen eszközökkel rendelkezik már a holland, és német haderő.

¹¹⁴ Németh András: Mobiltelefon hálózatok alkalmazása a katasztrófavédelmi kommunikáció területén, ZMNE Kommunikáció 2005

Egy bevásárlóközpont előtti parkolóban, majd 2 perc elteltével 700 m-rel odébb, egy metróállomás peronján nagy erejű pokolgép robban. Az első detonációt követően a helyszínre érkező járőrpáros miután felmérte a helyzetet, rádión, vagy annak „hibája” esetén mobiltelefonon értesíti az előljáró parancsnokot, vagy az eljárási szabályokban rögzített illetékes parancsnokot, aki meghatározza számára a feladatokat. Az előljáró értesíti az intézkedésre kijelölt rendőri szerveket, mentőszolgálatokat, a tűzoltóságot, a nemzetbiztonsági szakszolgálatokat, a tűzserészeket stb. Időközben bekövetkezik a második detonáció, amit az első helyszín felé úton lévő tűzoltóautó személyzete észlel és jelenti parancsnokának. Az tájékoztatja a rendőrség illetékes parancsnokát, aki gyors helyzetértékelést követően utasítja a mobilszolgáltatókat a HHVR 4. szintjének aktiválására, meghatározva az érintett körzeteket. A lekapcsolást megelőzően az üzemeltető SMS-t küld a körzetben tartózkodóknak és a rendszer összes előfizetőjének a foganatosított intézkedésekről és a javasolt magatartásról. (Ezzel jelentősen csökkenthetők a lakosság azon pánikreakciói, melyeket az információhiány okoz.) Ezt követően a fennálló összeköttetések megszakadnak és az „átlagos felhasználók” a körzetből induló, valamint az ide irányuló híváskezdeményezés esetén foglaltsági jelzést hallanak, míg a mentésben résztvevők minden szolgáltatáshoz „korlátlanul” hozzáférhetnek. Így a terroristák nem tudnak mobiltelefonos távirányítással újabb pokolgépeket robbantani a mentőalakulatok közelében. (Amennyiben fennáll a veszély, hogy esetleg más körzeteket is támadás fenyeget, a korlátozást a rendőrség javaslatára a „kormányzati megbízott” kiterjesztheti a város teljes területére.) A két vezeték nélküli távközlési rendszer együttesen ki tudja szolgálni a kommunikációs igényeket mindaddig, amíg az EDR üzemében zavarok nem lépnek fel. Ekkor ugrásszerűen megnő a mobilforgalom, amit a rendelkezésre álló kapacitások még a tartalék áramkörök aktiválásával sem tudnak folyamatosan kielégíteni. A „híradás” további biztosításának érdekében az illetékes parancsnok utasítására a kérdéses körzetekben a szolgáltatók ügyeletes karbantartó egységei tartalék (mozgatható) bázisállomásokat telepítenek.

A forgalom jelentős részét ugyan a hangátvitel teszi ki, azonban a hálózatok számos kiegészítő szolgáltatást biztosítanak a krízis kezelése során, melyek hasznosítására számos lehetőség kínálkozik:

- A számos halálos áldozat fényképét a rendőrök MMS-ben továbbítják a náluk talált papirokból nyert személyi adatokkal együtt a központi adatbázisba, ezzel meggyorsítva azonosításukat, a családok tájékoztatását és a későbbi adminisztrációt...
- A sebesültek osztályozása és ellátása lassan halad, mert a kialakult kaotikus forgalmi helyzetben a mentőalakulatok csak lassan tudják megközelíteni a helyszíneket, annak ellenére, hogy a körzeteket biztosító járőrök folyamatosan irányítják az érkező járműveket. A helyszínen tartózkodó elsősegélynyújtók és mentőápolók a súlyos, spe-

ciális sérülésekről (pl.: égési és csonkolásos sérülések) fényképeket küldenek az ügyeletes kórházaknak és specialistáknak, akik az információk birtokában előre tervezhetik a beavatkozásokat és a szükséges kezeléseket, ezzel jelentősen növelve a páciensek túlélés esélyeit...

- Az egyik helyszínt átvizsgáló tűzszerész egy gyanús csomagot talál a bevásárlóközpont bejárata mellett, majd a terület biztosítását követően megkezdí annak vizsgálatát. A csomagban talált szerkezet azonban számára még ismeretlen, ezért fotókat készít róla és elküldi azokat tapasztaltabb kollegáiknak, akik nemzetközi adatbázisokban és az Interneten próbálnak a feltételezett pokolgépről adatokat fellelni...
- Időközben a családtagjaikért, ismerőseikért aggódók a helyszínek közelében próbálnak információkhoz jutni a felállított mobil tájékoztatási központokban elérhető, folyamatosan bővülő adatbázisokból. (sebesültek, az őket fogadó egészségügyi intézmények, elhunytak stb.)...

Néhány óra elteltével a hatóságoknak sikerül a helyzet normalizálása, helyreáll a közrend és a közlekedés, a sérültek többségéhez időben eljutott a megfelelő orvosi segítség, így az idő múlásával nem nő tovább a halálos áldozatok száma. Elhárították az egységes digitális rádiórendszerben keletkezett üzemzavart, elbontják a tartalék mobil bázisállomásokat. A hatóságok döntése alapján inaktíválják az elsőbbségi hozzáférés-vezérlési programot (SMS-ben tájékoztatják a felhasználókat), visszaáll a 'normál üzemállapot' (0. szint), minden előfizető azonos prioritással telefonálhat...

A mobiltársaságok a szerződésekben foglaltak szerint „kiállítják a számlát” a korlátozás miatt keletkezett kár, és a készenléti szervek által generált forgalom alapján...

A fenti, kissé erőltetettnek ható példa azzal számolt, hogy a földi rádiótelefon hálózatok üzeme, és a HHVR keretén belül történő működése nem volt veszélyben, hiszen ehhez minden feltétel és körülmény adott volt. Fontos kérdés azonban az, hogyan biztosítható a védekezésben résztvevők híradása, ha valami miatt a földi telepítésű vezetékek nélküli hírközlő rendszerek nem vehetők igénybe a katasztrófa sújtotta területen...

Műholdas rendszerek szerepe és jelentősége a veszélyhelyzeti hírközlésben

2004. december 26-án Szumátra nyugati partjainak közelében elemi erejű (Richter skála szerint 9-es) földrengés rázta meg a Csendes óceán mélyét, melynek következtében óriási hullámok indultak meg a délkelet-ázsiai partvidékek felé. Az egyre sekélyedő mederben feltornyosult óriási víztömeg

szökőárként tarolta le 12 ország partvidékét, csaknem 300 000 áldozatot követelve, és több mint 5 km mélységben elpusztítva a teljes-, így a távközlési infrastruktúrát. A katasztrófa következtében nullára amortizálódott földi hírközlési rendszerek mellett a kommunikáció biztosítására egyetlen lehetőség maradt volna, a műholdas telefonok alkalmazása. Mivel a térségben ilyen berendezések (és előfizetések) nem álltak rendelkezésre, csaknem egy teljes napot kellett várni az első hívás létrejöttéig. Az INMARSAT¹¹⁵, a „Távközlés határok nélkül”¹¹⁶ karitatív együttműködés keretében, Sri Lankán nagysebességű műholdas távközlési vonalakat és koordinációs centrumot telepített, majd rövid időn belül hasonlókat hozott létre az ország több érintett településén is. A vonalak egy részét a mentésben résztvevők, másik részét pedig a polgári lakosság használhatta.¹¹⁷

Természetesen a szökőárakon kívül számos más veszély is fenyegeti a 21. századi földi telepítésű távközlési hálózatait úgy stacioner, mint mobil viszonylatban. Természeti katasztrófák tekintetében jelentős károsodást okozhatnak a földrengések, melyek a hírközlő rendszerek vezetékes és optikai vonalainak szakadásával, a vezérlő rendszerek és kapcsolóközpontok, valamint a mobilrendszerek adótornyainak pusztulásával fenyegetnek. (Emellett az energiaellátó hálózat sérülése is súlyos károkat okozhat a hírközlő rendszerekben.) A Magyarországot is súlyosan érintő ár- és belvizek elsősorban a földben húzódó távközlési és elektromos kábelekre jelenthetnek veszélyt, (azokat beázással fenyegetik), ugyanakkor a rövid idő alatt lezúduló jelentős mennyiségű csapadék által felduzzasztott patakok is jelentős problémát okozhatnak, amennyiben az útjukba kerülő hidakat elmosás, így megszakítva az azon keresztülhúzó vezetékeket és kábeleket. (Mindkettőre volt már példa hazánkban!) A globális éghajlatváltozás következtében hazai viszonylatban is jelentősen megnőtt az extrém erejű viharok és rendkívüli mennyiségű csapadékok valószínűsége. (A 2006. augusztus 20-ai tűzijátékot elsöprő, budapesti orkánerejű vihar kitörését követően több mobiltelefon szolgáltató hálózata is használhatatlanná vált több mint 30 perces időtartamra!) Ezen időjárási szélsőségek elsősorban a légvezetékeket, a mobiltelefon bázisállomások antennáit (bár ezek rögzítő mechanikáját extrém szélnyomásra tervezik) leszakadással, töréssel fenyegetik, azonban ilyen esetben is számolhatunk a kábelek beázásának következményeivel is.

A természet elemi erői mellett egyre növekvő veszélyt jelentenek a civilizációs eredetű veszélyforrások, a terrortámadások...

¹¹⁵ International Mobile Satellite Organization (korábban: International Maritime Satellite Organisation)

¹¹⁶ Telecom sans Frontiers

¹¹⁷ Maros Dóra: Távközlési hálózatok működésének nemzetközi és hazai szabályozási kérdései veszély- és katasztrófhelyzetekben (Doktori értekezés tervezet), 2006

A távközlési rendszerek (a mobiltelefon hálózatokat is ide értve), mint a kritikus infrastruktúra¹¹⁸ részei kiemelt szerepet töltenek az egyes országokon belüli és a nemzetközi gazdasági, társadalmi, politikai életben, és mindennapjaink elengedhetetlenül fontos részévé váltak. Ez a kommunikációs függőség jelenti a legnagyobb veszélyt a modern társadalmakra, és teszi vonzó célponttá egyes terrorista csoportok számára. Az információs terrorizmusnak tehát nem csak eszköze, hanem céljai is lehetnek a kommunikációs infrastruktúra elemei, melyek működésképtelensége viszonylag gyorsan és akár hosszú időre is megbéníthatja teljes országok mindennapi életét, megrendítve azok gazdaságát, társadalmi bizonytalanságot okozva, félelmet keltve az emberekben. Az információs támadásokat a végrehajtás módszere alapján két csoportba sorolhatjuk. A *fizikai támadások* egyes rendszerelemek megsemmisítésével, működésképtelenné tételével, míg az *információs támadások* szoftveres úton 'logikai rombolással' érik el, hogy adott területen ne legyenek hozzáférhetők a hírközlő hálózat (hálózatok) szolgáltatásai. Az első csoportba a hagyományos terrorizmus fegyvertárába tartozó - például robbantással végrehajtott -, a kapcsolóközpontok, bázisállomások, hálózat-felügyeleti- és vezérlőrendszerek, valamint az átviteli utak ellen irányuló támadások, vagy azok energiaellátását biztosító rendszerek 'kiiktatása' tartoznak. A második csoportba tartozó módszerek azt használják ki, hogy a 21. század hírközlő hálózatai óriási globális rendszert alkotnak, számtalan kapcsolódási felülettel más távközlési, valamint informatikai hálózat (pl. Internet) felé, valamint hogy ezen hálózatok irányítása, felügyelete szintén számítógépes rendszerekkel történik. Ezekbe - az informatikai, vagy fizikai biztonsági rendszereket kijátszva - szoftveres, vagy hardveres úton behatolva lehetőség nyílik az adatbázisokban tárolt információk, manipulálására, hozzáférhetetlenné tételére (pl. előfizetői adatbázisok, azonosítók), vagy a rendszer vezérlésének megváltoztatására akár oly módon, hogy az egyes hardverelemek fizikailag is károsodjanak.

A legnagyobb probléma persze akkor jelentkezik, ha valamilyen katasztrófa helyzet idején következik be (akár azzal szoros, ok-okozati összefüggésben) a földi hírközlő rendszerek károsodása, hiszen ekkor jelenősen romolhatnak a védekezés hatékonyságát biztosító vezetés és irányítás kommunikációs feltételei. Problémát jelenthet például hogy számos esetben költséghatékonysági szempontok alapján az egyes mobil rendszerek bázisállomásai és antennái ugyanazonokon a helyeken és infrastruktúrákon (pl. tornyokon) kerültek elhelyezésre, ami együttes (azaz több szolgáltató egyszerre történő) fizikai sérülésük valószínűségét jelentősen növeli. (A Magyarországon kiépítés alatt

¹¹⁸ Azok az infrastruktúrák, melyek rendeltetésszerű folyamatos működése elengedhetetlenül fontos a többi infrastruktúra működéséhez. (pl. energia termelő és ellátó rendszerek, köz-, és vasúthálózatok, repülőterek, kikötők stb.)

álló EDR rendszer antennái sok esetben a T-mobile, míg máshol a BM¹¹⁹ tornyai kerültek elhelyezésre!) Másik veszélyforrást a tartalék áramkörök, a működőkkel azonos infrastruktúrán történő kialakítása jelenti, ami adott hálózaton belül mehet a működőképesség rovására kritikus helyzetekben.

Jelen állapotok szerint a magyarországi készenléti szervek nem rendelkeznek, olyan hírközlő rendszerrel, amely biztosítja akár a belső, akár az együttműködési híradást, a földi hírközlési infrastruktúra jelentős sérülése esetén.

Ezeket a szempontokat figyelembe véve szükséges egy, a földi mobil távközlési hálózatoktól függetlenül is működni képes, alternatív kommunikációs lehetőség rendszerbe állítása, ami adott esetben gyorsan installálható tartalékként, ha jóval szűkebb keresztmetszetben is, de képes biztosítani a veszélyhelyzeti híradást az ország egész területén! Ezen feltételrendszernek a műholdas mobil hírközlő rendszerek megfelelnek, hiszen ezek működtetéshez, szolgáltatásaik igénybevételéhez Magyarországon nincs szükség semmilyen földi infrastruktúrára, csak és kizárólag a megfelelő „előfizetésekre” és végbevezetésekre.

Magyarországon jelenleg (1996 óta) a Magyar Honvédség rendelkezik bérelt műholdas és előfizetői kommunikációs csatornákkal, melyek nélkül külföldi kontingenseivel történő kapcsolattartása nem, vagy csak nehezen lenne biztosítható. (A hadművelleti területeken néha ezzel biztosítják az alegységek híradását is.) Az igénybe vett INMARSAT, Iridium és VSAT¹²⁰ szolgáltatások eddig igazolták a velük szembeni várakozásokat és folyamatos, megbízható kommunikációt biztosítottak.

A műholdas távközlési rendszerekkel eddig szerzett tapasztalatok igazolták, hogy az általuk nyújtott szolgáltatások segítségével bonyolultabb műveletek híradása is biztosítható, így kiválóan alkalmasak akár a katasztrófavédelmi feladatok kommunikációs támogatására is.

VSAT rendszerek segítségével lehetőség van akár diszpécser jellegű zárt célú (virtuális) hálózat(ok) létrehozására is, amelyben a beszéd és adatátviteli szolgáltatások rugalmasan optimalizálhatók a végrehajtandó feladatokhoz. A védekezési munkálatok irányításához létre kell hozni olyan Mobil Vezetési Pontokat (gépjárműbe szerelt), melyek képesek a központi állomás szerepét betölteni (HUB), és a melyek az egyes együttműködő szervezetek vezetési pontjaival, valamint a végrehajtó csoportok irányítóival állnak összeköttetésben, valamint biztosítják a kommunikációs csatornákat külföldi társszervek felé (gerinchálózat). (A gerinchálózat tartalékát speciális INMARSAT terminálokkal lehet megvalósítani.) Az alárendeltek, a munkálatokban résztvevők vezetését Iridium és INMARSAT műholdas telefonokkal lehet biztosítani. (A

¹¹⁹ egykori Belügyminisztérium

¹²⁰ Very Small Aperture Terminal

fenti szolgáltatók alternatívájaként lehetőség van más rendszerek igénybevételeire is, mint például a THURAYA, amelynek szintén vannak „katasztrófavédelmi referenciái”). A műholdas rendszerek segítségével lehetőség nyílik számítógépes hálózatok összekapcsolására, adatbázisok elérésére, valamint akár az INTERNET-re történő csatlakozásra is.

Összegzés

Cikkemmel a jelenlegi helyzetből kiindulva szerettem volna bemutatni, hogy bár jó irányban és dinamikusan halad hazánkban a veszélyhelyzeti hírközlés fejlesztése, az nem képes lépést tartani az új kihívásokkal. A jövő szempontjából mindenképpen fontos, hogy bizonyos lépéseket ne utólag, egy jelentős katasztrófa (számos áldozat és jelentős anyagi kár) bekövetkezését követően tegyünk meg (mint például a 2006. augusztus 20-ai vihar esetén), hanem előre gondolkodva felkészüljünk a váratlan helyzetek kezelésére is. Ezt a hírközlés területén az általam javasolt többszintű rendszer bevezetésével, a különböző földi és műholdas mobil szolgáltatók rendszerei által kínált szolgáltatások rugalmas igénybevételel lehet elérni, ami nagyban segítheti a természeti katasztrófák, ipari balesetek, terrorcselekmények következtében kialakuló krízishelyzet megelőzését, illetve kezelése során az érintett hatóságok, szervezetek és szakemberek együttműködését.

Felhasznált irodalom:

1. NÉMETH András, Dr. habil Sándor Miklós: *A katasztrófavédelmi kommunikáció jogi szabályozása Magyarországon* – ZMNE, Budapest, Kommunikáció 2004
2. András NÉMETH, András Somos: *Emergency Communications Systems in the United Kingdom*, AARMS Vol. 4, No. 2, 2005
3. NÉMETH András: *Mobiltelefon hálózatok alkalmazása a katasztrófavédelmi kommunikáció területén* – ZMNE, Budapest, Kommunikáció 2005
4. PÁNDI Erik: *A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai- és közigazgatási kommunikációs rendszerek megszervezésére és irányítására (Doktori értekezés tervezet)* – ZMNE, Budapest, 2005
5. FEKETE Károly: *A Magyar Köztársaság kommunikációs infrastruktúrája (Egyetemi jegyzet)* – ZMNE, Budapest, 2004
6. DÉRFÖLDI László, Pintér István (Szerk.): *A Honvédelmi felkészülésre, Nemzetbiztonságra, Polgári Védelemre, Katasztrófavédelemre, Titokvédelemre vonatkozó és a NATO tagságból adódó fontosabb Jogsabályok* - Hírközlési Felügyelet, Budapest, 2003
7. MAROS Dóra: *Távközlési hálózatok működésének nemzetközi és hazai szabályozási kérdései veszély- és katasztrófa helyzetekben (Doktori értekezés tervezet)* – ZMNE, Budapest, 2006

8. MÁTÉ József: *A katasztrófavédelem infokommunikációs támogatottsága* – ZMNE, Budapest, Kommunikáció 2005
9. MAROS Dóra, MÉSZÁROS Árpád: *A magyar távközlési rendszer anomáliái a londoni terrortámadás tükrében* – ZMNE, Budapest, Kommunikáció 2005
10. KOVÁCS László: *A terrorizmus veszélye és a Magyar Köztársaság kommunikációs infrastruktúrája* – ZMNE, Budapest, Kommunikáció 2005
11. Nemzeti katasztrófavédelmi Stratégia (<http://www.katasztrofavedelem.hu>)
12. Mobil Gyorsjelentés 2006. június - NHH (Nemzeti Hírközlési Hatóság)
13. Emergency Events Database (EM-DAT) (<http://www.em-dat.net>)
14. Borough of Barking and Dagenham, Emergency Plan-Communications, Appendix 3, September 2004.
15. Wireless Week-UK Networks On New Year's: Too Loaded, Jan 10,2000

Schuller József Attila:
Mobil munkavégzési megoldások a Kapschtól
Kapsch Kft termék marketing menedzser

Kapsch Kft. | kapsch >>>

Mobil munkavégzési megoldások a Kapschtól

Schuller József Attila termék marketing menedzser
Kapsch Kft.



Kapsch Kft. | kapsch >>>

Hol vannak a dolgozók?

OTTHON



ÚTKÖZBEN



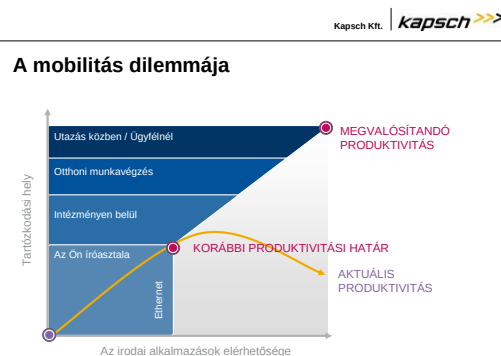
VALAHOL HÁZON BELÜL



A munkavégzéssel kapcsolatos igények azonban nem változtak...

- > Kapcsolatba lépni
- > Az információkat elérni
- > Egyre mobilabbá válni

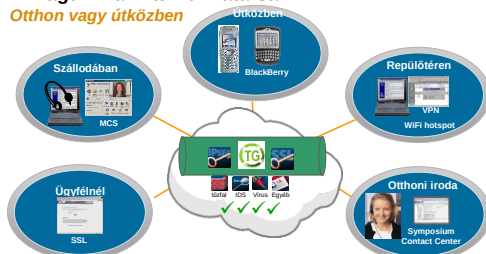






A magunkkal vitt munkatársak

Otthon vagy útközben



Nagyobb produktivitás a biztonságos elérési technológiákat használó multimédiás alkalmazások és kliensek révén

Multimedia Communication Server 5100

A valós idejű csoportmunkát támogató alkalmazások

- > Funkciókban gazdag multimédiás üzleti alkalmazások
 - A SIP lehetőségeit használja ki
 - Hálózati alapú, elosztott szerver kliens felépítésű architektúra
 - Szabványos platformok



A felhasználó által élvezett előnyök

- > Mobilitás
- > Csoportmunka alkalmazások
- > Produktivitás és személyre szabás
- > Integrált felhasználói élmény
- > Beruházásvédelem

Új multimédiás kommunikációs és csoportmunka szolgáltatások az intézmények számára

Még több csoportmunkát támogató eszköz

> Integrált kommunikációs és csoportmunkát támogató eszközökkel gazdagítja a beszélgetést és javítja a produktivitást



Mobilitási megoldások használata a Nortelnél

- > Több mint 21.000 hordozható PC-vel rendelkező alkalmazott bárholonnan biztonságosan éri el a beszéd- és adatátviteli alkalmazásokat (az MCS-t és VPN-t használva)
- > Eredmények:
 - > A mobil, távolsági és helyi telefonköltségek csökkentek, mégpedig **52%-kal** a felső vezetők, **42%-kal** az értékesítési megbízottak, és **90%-kal** az otthon dolgozó távmunkások esetében
 - > A távmunkásoknak köszönhetően a Nortel évi **22 millió \$-t** takarít meg az ingatlanköltségekben
 - > A dolgozók produktivitása közel **15%** javulást mutat



Miért az MCS 5100 webes csoportmunka a távmunkát/távoktatást elősegítő fő alkalmazás?

Átalakítja a távmunka végzésről alkotott képet

- > Valós idejű többfelhasználós webes csoportmunka
- > Integrált csoportmunka megoldás
 - Audio és videokonferencia, IM cset és további funkciók
- > Mindig elérhető
- > Költséghatékony



MCS 5100 webes csoportmunka

> Dokumentum közzététel

- MS Office dokumentumok prezentálása

> Alkalmazás megosztás

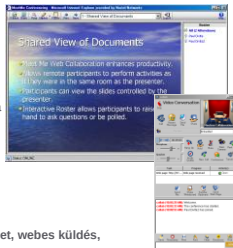
- Bármely dokumentum, alkalmazás, vagy a teljes képernyő megosztása
- Dokumentumok szerkesztése valós idejű módon

> Szavazás

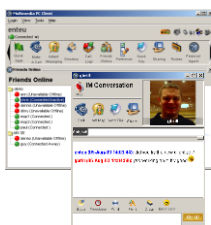
> Fájlok küldés

> Valós idejű csoportmunka

- Jelenlét, azonnali üzenetküldés, cset, webes küldés, értesítés azonnali üzenetküldéssel



Gazdagítsuk virtuális értekezletünket az MCS 5100 csoportmunkát támogató alkalmazásaival



> Jelenlét

- Egyetlen pillanattal megállapíthatjuk a leendő résztvevők elérhetőségét (pl. online, off line, telefonál)

> Azonnali üzenetküldés és csetelés

- Mások számára észrevétlen módon kaphatunk azonnali választ kérdéseinkre – valós idejű kommunikáció

> Videó

- Visszahozza a szemtől szembeni kommunikáció élményét a távmunkások számára

> Fájlok küldés

- Multipont fájlok küldés a webes együttműködési ablakból

Összefoglalás

> Valós idejű SIP-alapú multimédiás kommunikációs szolgáltatások

- Mobilitás
- Csoportmunka alkalmazások
- Produktivitás és személyre szabás
- Integrált felhasználói élmény

> Előnyök

- Gyorsabb, gazdagabb kommunikáció
- Produktivitás növelés
- Pénz megtakarítás

> Átalakítja a meglévő kommunikációs formákat

- Előre tervezhető kommunikáció
- A kommunikációs médiumokhoz illeszkedő szolgáltatások
- Kritikus információk pont időben történő elérése



Összefoglalás (folyt.)

> Bevezetési lehetőségek

- Saját rendszer implementálása
- Szolgáltatás vásárlása a Kapschtól



Köszönöm a figyelmet!

Schuller József Attila
jozsefattila.schuller@kapsch.net



Gábor Egri

Information technology in policing in the european union
the schengen information system

1. Introduction, the information technology in policing activities

The police work, similarly to any other activity, requires a lot of resources for itself. One of them is the information technology (IT) which has huge importance nowadays in consequence of its technical level. The general usage of IT can increase the effectiveness of everyday activity and has some special features, as it can reduce the necessity of other resources.

The special role of IT in the police work and between their needs, the conversion of necessary resources will be explained in the following points.

- The IT and telecommunications, as serving activity to police work and as universal resource

The IT and telecom activity is used widely in every place of social life and economy. The situation is similar in every-day police work as the state-of-the-art computer technology and other possibilities are widely used nowadays in public administration. For instance the electronic mails, the telephone and fax connections have decreased the volume of the conventional mails and flowing of documents.

Information are significant and very important resources for the police work, so information-technology as the science dealing with the creating, processing, transmission and evaluation of information has a huge relevance in the professional work.

- Police IT in local, regional, nationwide and international level (SIS)

In the beginning the practice in the work of police proved the usefulness of local bases of information. Afterwards every separate organisation started to create and later enlarged their info, so this scheme became to operate as a real database. Nowadays the fight against cross-border crime need in incredible level the international interoperation of the police organisations and it is effectively and at this moment irreplaceably served by special European information system, by the Schengen Information System (SIS).

The present work deals with SIS in operation and under development.

2. Short historical overview

The Schengen Agreement was signed on 14th of June, 1985 by Belgium, France, Germany, Luxemburg and The Netherlands. Its main goal was to ensure the free movement of goods, persons and services throughout their common border. On 19th of June, 1990 the Convention was signed implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. The Schengen Convention has clearly defined the detailed rules to implement into practice the sense of these acts.

In the nineties of the last century ten European countries joined the Convention gradually, eight of them from the European Union, Italy, Spain, Portugal, Greece, Austria, Denmark, Finland, and Sweden, and as not member states of the EU, Norway and Iceland.

The Schengen acquis were published in the Official Journal of the EU, based on the 1999/435/EC Council Decision of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis.

The necessity of a common cross-border communication system came out clearly from these documents.

Article 44 of the Convention, implementing the Schengen Agreement says:

“1. In accordance with the relevant international agreements and account being taken of local circumstances and technical possibilities, the Contracting Parties shall install, in particular in border areas, telephone, radio, and telex lines and other direct links to facilitate police and customs cooperation, in particular for the timely transmission of information for the purposes of cross-border surveillance and hot pursuit.

2. In addition to these short-term measures, they will in particular consider the following options:

- (a) exchanging equipment or posting liaison officers provided with appropriate radio equipment;*
- (b) widening the frequency bands used in border areas;*

- (c) *establishing common links for police and customs services operating in these same areas;*
- (d) *coordinating their programmes for the procurement of communications equipment, with a view to installing standardised and compatible communications systems.*" [SchConv]

The first generation of the Schengen Information System started its operation in March 1995 after thorough-going analysis of technical, legal, economical, and financial aspects of development. As a consequence of it the way through between the common frontiers of contracting parties became free-crossing for travellers without any border control.

The data-transport network for the data-connection purposes between the countries, the SISNET began to run in 2001.

The system serving 15 countries has been developed in several functions during its work so it is called SIS 1+ now. The current system has 15 participants but it is a coincident only by chance with the numbers of the former member states of the EU. The United Kingdom and Ireland are not part of the system, but Norway and Iceland, as out of EU members are in.

The ten new member states acceding to the EU on 1st of May 2004 shall fulfil the Schengen requirements by the Accession Protocols and Agreements to the 1985 Agreement and the 1990 implementing Convention (signed in Athene). The European Commission will enlarge the SIS to make the opportunity to ensure the Schengen accession for them. The brand new system, the SIS II will enable the joining for all member states and for Switzerland, too. The call for tender for the development of the new system was published in August 2003 and the dead-line for the project was settled as March 2007.

In the author's opinion the SIS II will serve to this deadline only such functionalities like the SIS 1+ operation and will allow the joining of new countries the central system. The integration of the separate nations will follow a step-by-step procedure after the Schengen evaluation process. New features like biometry will only appear gradually in the near future led by the development of technology. These new ones, as surveying, processing and searching of data (fingerprints, palm-prints, pictures, images, etc.) will increase very much the effectiveness of the whole system.

3. The system

The structure of the system can be seen in figure 1. It shows four different main elements of the operation, as:

- C. SIS Central database and operational staff of the Schengen Information System;
- N. SIS National system including national copy of the database;
- SISNET International transport network between the central and national systems;
- Internal network of member states.

The N. SIS and the internal network are slightly different country-by-country fitting into the national specialities of the states, e.g. the federal structure of the land or the supervision of the police etc. But there are essential conformities in every country that on the one hand can be isolated a technical apparatus dealing with the operation and maintenance of the system and on the other hand an administrative unit, so called SIRENE office holding together and organising the international connection of the changes of police information. The SIRENE office has the proper rights to function as an intelligent interface between the different countries.

Nowadays the N. SIS in operation in every state contains the national copy of the central database which enables the reliable running of the system and ensures the safety copy of the data in the whole structure. So every national database consists of two types of data: one of them contains the so called Schengen data with decreased amount of information and the other one is the register of the whole national info.

The operation of the system

The operation of the system can be followed by figure 2. In accordance with the illustration the end user (e.g. the border police officer) in his/her service place enters the data to be controlled into the system. (This interface is more or less a computerised check point including a document reader.) After putting data in the system will generate a hit/no hit answer and the officer's process is led by this answer. The no hit position means that the system does not contain any flag in the registers in connection with the person in question.

When a SIS search is successful, i.e. the asking party has got a positive answer additional information could be required. It can be handled only throughout the SIRENE office and the information is exchanged bilaterally between SIRENE bureaux.

If so, the worker of the SIRENE office of the data asking party gets in touch with the SIRENE officer of the data entering country who the source of the information is. The following steps depend on this. So we can see that the

SISNET is not only the transport network of data transmission but it has a big role in the voice and fax connections between the SIRENE bureaus, too.

4. The usage of the system

The use of the system is in very close connection with the IT and the police activity including the whole territory of the interested parties. Of course this activity will gradually extend to all member states of the European Union depending on the preparedness of the countries. The most spectacular application of the system is the border control as it is the best known adoption for the public. This opportunity can be divided into several parts depending on where the operation is in use.

4.1. Usage at external border

The SIS is in use at external border as an IT support to border police and customs. (External border means a border between countries where one country is the member of the EU but the other is not. So in every case an international airport or harbour is external border even if its traffic is moving not only within the EU.)

Just such detailed control, based on all the data of the Schengen countries can guarantee the high level inner safety of the European Union. The officer of the public administration in the external border protects not only his/her own country but the whole Schengen area.

4.2. Usage at inner border

Just upon the total control at the external border is possible to eliminate the border control at the internal borders, at the common borders of the states that signed the Schengen Agreement. In such cases the open frontier is realised without any stopping and difficulties, the border crossing is known only by seeing the foreign language text.

So the SIS applications at the inner borders can be seen as a special use of IT support applied in the other places of the EU, at the external borders.

4.3. Other applications

Other applications of the SIS are the cases when the police make the so called in-depth control, the supervision made in the inner part of the country by border police. This police activity has rising importance due to the problems of migration, smuggling and organised crime. In this case the officer makes his/her duty in the whole territory of his/her region using necessarily the IT resources of SIS, as in the case of a real border control.

The other special application is the loading of the data bases when the appropriate officer who has proper right for data procession deals with the posi-

tioning of flags into the SIS database upon the legal decisions with consequences. This process is mainly a legal one and it is out of the boundaries of the present work.

To summarise the applications of SIS we can explain a so called Schengen area where the free movement of persons, services and goods is achieved. Real border control is made only at the external borders of the community. The police of each country are working by their own legal bases in their territory but the necessary information is exchanged by them.

5. Development of the system

The Schengen Agreement and the Schengen Convention was signed more than 15 years ago and the SIS has begun its running for more than ten years. The development of the technical level of IT was increased significantly and the political environment changed a lot during this period of time so the Commission of the EU decided to fundamentally reconstruct the present system, to create the second generation Schengen Information System, the SIS II.

5.1. The necessity of SIS II

During the development process the European Commission started to set up a brand new system. The necessity of it is based on the following aspects:

- The present so called SIS 1+ system is ready to serve only 18 countries. This figure was counted as the total number of former and old member states (15) and the number of potential parties, Norway, Iceland and Switzerland. The accession protocol of ten new countries contains that it is obligatory them to use the Schengen Acquis and to join the Schengen area. To fulfil this obligation the EU as the admitting organisation has to prepare its technical system itself for this task.
- Since starting the operation of SIS the IT has been developed very much the digital technology has spread in general use in computer science. Mentioning only the main aspects of these developments nowadays the mobile communications reached incredible high level, together with other elements serving the mobility, the capacity of memories and computers increased rapidly, the speed of data communication grew up several times as before, etc.
- It is necessary to enlarge the connecting capacity not only because the number of member states increased but new international organisations, as Europol, or Eurojust appeared as potential end-users of the information system. The accession of EU made in 2004 and the number of acceding countries and other organisations will resume even more than 30 connecting parties instead of the present 18. This procedure of

course is not only a technical task but has a lot of legal problems to solve in the near future, too.

5.2. Main features of SIS II

The present services of the SIS suffered larger and smaller developments several times during its operation. These new implementations meant the enlargement of services and more powerful applications but the architecture of the system is the same as was before. The result of the new development will be the SIS II and it will fulfil a lot of new services respectively to new requirements. The Commission is responsible for the whole process of renewal of SIS.

- The process of the development is based on brand new platform of architecture. It means a modified conception with new elements of the system e. g. in the question of national copy. (It will be explained later.)
- A really new function is the more detailed data in the registers. So they contain not only alphanumeric characters but pictures, images, biometrics etc. ensuring more complex data processing possibilities.
- SIS II is in principle the newest IT system with much more power and robustness for serving better the end-user's requirements.
- The SIS II made a big step forward to enlarge the basis of information (e. g. biometrics) and using this platform to process data and support new European legal tasks as EAW (European Arrest Warrant).
- The possibility of interconnections between the SIS and VIS systems enables more efficient way to fulfil the interests of the member states.
- The new system brings closer to the optimum the use of national and communal resources. To compare to the present operation the network management, the operation and maintenance, testing of the system, change management will be simpler and so it will increase cost efficiency. The up-to-date positions, the scalability, the easier management will lead to use a more resilient system ensuring the maximum capacity and effectiveness.

5.3. The structure of SIS II

The new structure of SIS II is very similar to the one on the figure 1 but this analogy is only superficial. The four elements can be represented as follows, changing C. SIS to CS and N. SIS to NI:

- CS Central system is the central database of the Schengen Information System with proper redundancy and back up system
- NI National interface to contact the member state to CS

- International backbone network for voice and data communications instead of SISNET
- Internal network within the member states

The inner meanings of the elements are rather different and complex. It contains a lot more than the present SIS 1+ system.

The CS is the heart of SIS II, it must be able to guarantee that data putting in via the national interfaces is validated, stored and safely delivered to all national interfaces for all member states.

The NI is an identical system-to-system interfaces where all SIS data is inserted by the country/user that owns the data, and where all the data in the SIS become accessible. The main difference between the NI and N. SIS is that the national interface does not include the functionality of national copy. It works only as a complex interface between the central data base and the member state. The loading of data is done throughout this surface and the searching algorithm is working similarly through, too. Optional services could be provided by the interfaces, too.

In the new system the national copy is not used in every member state. It is typical that the old member states having the national copy now will preserve for themselves the possibility of own copy on the basis of the present storages. This opportunity is unnecessary and results needless additional charges by the Commission. Hungary does not plan to create national copy. In consequence of absence of a national copy the reliability, redundancy and back up of the central system shall be realised in much higher level than the present one. The working centre of CS is in Strasbourg, France and the back up system will be located in Austria.

Another significant difference is the speed of data transmission in the network. Nowadays the technical possibilities are much greater than at the beginning of the operation were, so the new network will be able to serve the higher requirements in the field of security, safety and the strong volume of information.

The main functions of the new structure and the division of responsibilities are shown on the figure 3.

6. Setting up the SIS II system

The time schedule of the creation of the SIS II system is a very important political issue in the EU. The beginning of 2007, as the deadline for the going

into operation was decided in the beginning. The call for tender was issued in August 2003 but the legal procedure followed by the evaluation has stopped the process for several months. After the consensus the development could continue but the official deadline was not modified seriously, by now it is April 2007. (Just in the last days there were some articles on the net about the postponement for 2008 but these are not official information.) Different process must be done by the old and new member states for joining the new system. First the old member states operating the present system have to migrate i.e. switch over from the old system to the new one. This procedure needs about 6 months including the testing and data conversion, too. Successful migration can be followed by the integration of new countries by new member states. It is interesting that the United Kingdom and Ireland not being members of the Schengen area at present have to do the similar integration process as the newly joining countries. Hungary wants to join the Schengen area in October 2007 under the governmental decision 2328/2004 (XII. 21.). Considering the practices of former accessions the real opening of the borders can be realised after several months following the readiness of the technical systems. E.g. the situation with Italy was the following: Signing the Agreement on the Accession of the Italian Republic to the Convention implementing the Schengen Agreement were done on 27th November 1990; the technical system was ready to use in 26 October 1997 and the opening of border were done at the beginning of next year.

Bibliography

[SchAgr] Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. Official Journal of the European Communities 22. 9. 2000

[SchConv] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. Official Journal of the European Communities 22. 9. 2000

Agreement on the Accession of the Italian Republic to the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their

common borders signed at Schengen on 19 June 1990. Official Journal of the European Communities 22. 9. 2000

Decision of the Executive Committee of 7 October 1997 on bringing into force the Convention implementing the Schengen Agreement in Greece (SCH/Com-ex (97) 29, rev. 2). Official Journal of the European Communities 22. 9. 2000

1999/435/EC: Council Decision of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis Official Journal L 176 , 10/07/1999 P. 0001 - 0016

Figures

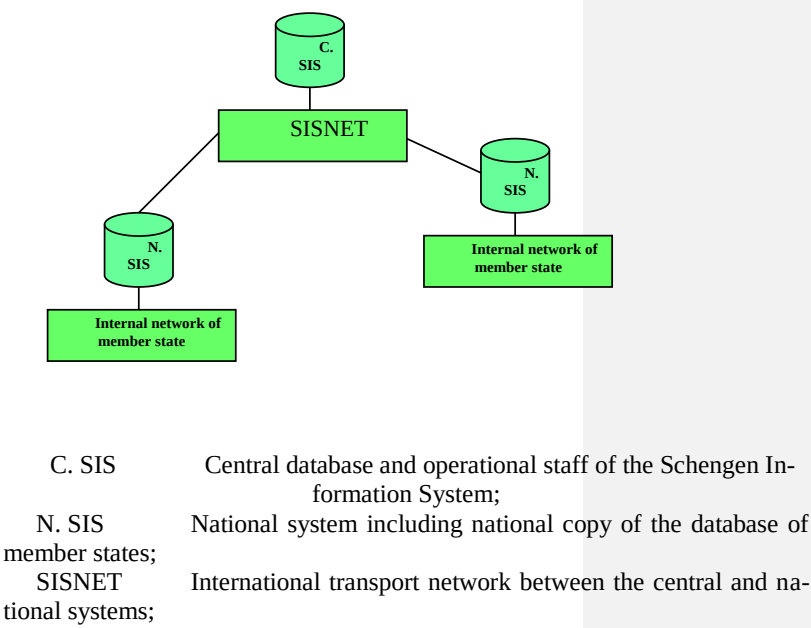


Fig 1. The theoretical structure of the first generation Schengen Information System

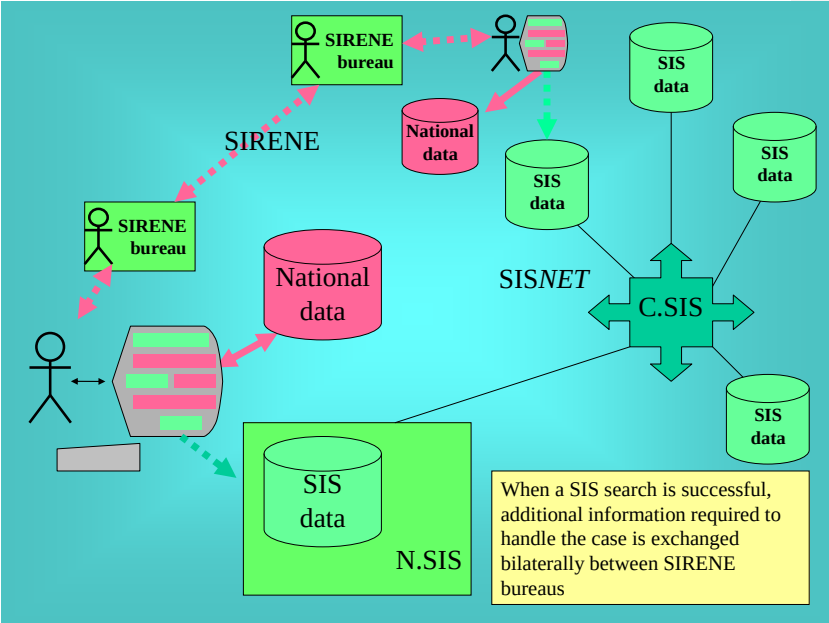


Fig 2. Flow of information in the Schengen Information System

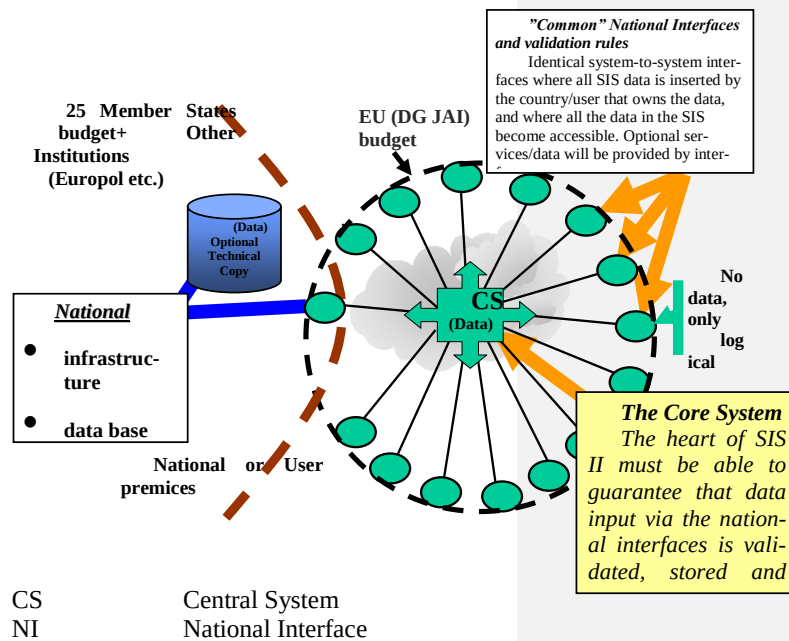


Fig 3. The share of responsibilities in the second generation Schengen Information System

Révész Gyula mérnök alezredes

A kor kihívásai a kiképzők szemével

Mottó:

„Egy háborút nem lehet megnyerni csak a technikai eszközökkel és a fegyverzettel, de meg lehet nyerni azokkal a katonákkal, akik alkalmazzák azokat. Még a legjobban felszerelthadsereg sem képes győzni motivált és jól felkészített katonák nélkül.”
FM21-75

Napjainkban a világ és hazánk biztonságpolitikai környezete – talán korábban soha nem látott gyorsasággal – változik és alakul át. A sorozott, állampolgári kötelezettségen alapuló hadseregek kora lejárt. Magyarország 2004. november 3-án végleg szakított egy 136 éves tradícióval: békeidőben megszüntette a sorozás intézményét, áttért a hivatásos és szerződéses katonákból álló haderőre.

Az önkéntes haderőnek olyan személyi állománnyal kell rendelkeznie, melyben a tisztek és a tiszthelyettesek mellett kiválóan felkészült, megfelelő tudással rendelkező szerződéses katonák teljesítenek szolgálatot. Olyanok, akik képesek a kihívásoknak eleget tenni akár hazai, akár nemzetközi műveletekben való részvétel során.

A kiképzők számára komoly kihívást jelent a szerződésesek komplex felkészítésében való szerepvállalás. Ennek folyamán valóban meghatározó szerepet játszhat az eddig oly sokszor csak hangzatos szólamként értékelt „parancsnoki példamutatás”.

A folyamatban lévő katonai oktatási reform, valamint a NATO tagságból eredő, megnövekedett követelmények, szükségessé teszik a tiszthelyettesekkel, mint a kiképzést közvetlenül végrehajtókkal szembeni elvárások megfogalmazását. Véleményem szerint hogy a fent említett elvárásoknak eleget tudjanak tenni az alábbi kritériumoknak kell megfelelni:

Követelmények megfogalmazása

Általános képességek, elvárások a kiképzővel szemben:

Alapvető és meghatározó elvárás a hazához és a nemzethez való feltétlen hűség, a politikamentesség, a katonai szimbólumok és az egyenruha iránti tisztelet, valamint a katonai hivatás iránti elkötelezettség.

A kiképző rendelkezzen:

- megfelelő fizikai, pszichikai felkészültséggel,
- katonai professzionizmussal,
- döntés előkészítő, döntéshozói képességgel,
- megfelelő vezetői ismeretekkel,
- karrier orientációval,
- képességgel mások érdekeinek képviselésére,
- az önművelődés, önképzés igényével,
- kommunikációs képességgel,
- elhivatottsággal hivatása iránt.
- pedagógiai ismeretek

A híradó tiszthelyetessel mint kiképzővel szemben támasztott követelmények:

Általános műveltség és általános katonai ismeretek területén:

A tiszthelyettes képző iskola eredményeként ismerje:

- a magyarság történetét, ezen belül hadtörténelmünk főbb eseményeit.
- a katonai híradás fejlődésének főbb mozzanatait, a magyar katonai és polgári híradás fejlődéstörténetét.
- a Szolgálati törvényt és a Hadköteles katonákkal kapcsolatos törvényeket, legyen képes e jogszabályok előírásainak gyakorlati alkalmazására.
- a Magyar Honvédség feladatát, felépítését.
- a Szárazföldi Parancsnokság szervezetét, alárendeltjeit, azok feladatait, a parancsnokság vezetési rendjét.
- a nemzetközi hadijog legfontosabb előírásait.
- a NATO feladatát, főbb szervezeti elemeit, tagállamait.
- a NATO tagállamok hadseregei által használt katonai rendfokozatokat, fontosabb beosztásokat és megszólításokat.
- a kiépített és kiépítésre kerülő védelmi építmények (pl.: EÁP-ok, óvóhelyek, tüzelőállások, vezetési pontok,) telepítésének rendjét, használatát, berendezéseinek alkalmazását.
- legyen képes az elfogadott társadalmi etikett szerinti megjelenésre, megnyilvánulásokra

Rendelkezzen:

- általános katonai ismeretekkel és készségekkel.
- általános ismeretekkel a békemissziós tevékenységekről.
- „B” típusú nemzetbiztonsági ellenőrzéssel.

- minimum alapfokú állami nyelvvizsgálattal vagy STANAG. 1. 1. 1. 1. nyelvvizsgálattal
- minimum „B” kategóriás jogosítvánnyal, állomásparancsnokok esetében javasolt a „C” kategóriás jogosítvány.

Legyen képes:

- az egyéni lőfegyverek készség szintű kezelésére.
- a személyi számítógép használatára, ismerje a WORD és EXEL programcsomagok alkalmazását.
- az alapvető híradó eszközök kezelésére.
- a munka és környezetvédelmi előírások gyakorlati alkalmazására és azok betartásának megkövetelésére.
- szakasz, raj szintű szervezet általános és szakmai (híradó) kiképzésének vezetésére.
- szakasz, raj szintű adminisztrációs tevékenység végrehajtására.
- híradó technikai eszközök álcázásával kapcsolatos feladatok irányítására, végrehajtására.
- fizikai felkészültsége olyan szintű legyen, hogy a fizikai követelményeknek legalább megfelelő szinten eleget tudjon tenni, legyen felkészítve az alapvető önvédelmi fogások alkalmazására.
- pedagógiai és katonai vezetői felkészültsége tegye lehetővé szakasz, raj szintű szervezet vezetését.
- a szolgálati, az alaki szabályzat és az öltözködési utasítás előírásait ismerje és legyen képes azok gyakorlati alkalmazására.
- tudjon szabályosan parancsot és vezényszavakat kiadni, azok végrehajtását megkövetelni.
- Legyen felkészülve a NATO szabványú térképek használatára, legyen tisztában az alapfogalmakkal.
- sajátítsa el a NATO rendszerű térképeken használt jeleket, jelöléseket, jelkölcsöket, valamint a különböző feliratokat, rövidítéseket azok alkalmazását.
- az ön-és kölcsönös segélynyújtás készségszintű végrehajtására úgy legyen kiképezve, hogy azt a gyakorlatban alkalmazni tudja. Legyen képes a legfontosabb életmentő beavatkozások gyakorlati végrehajtására, szükségeszközökkel és az egyéni egészségügyi csomag segítségével tudja megkezdeni a sérültek első ellátását.

Általános híradó szak követelmények híradó tiszthelyettesek kiképzők részére:

- ismerje a híradó szolgálat rendeltetését, fő területeit, helyét és szerepét Magyar Honvédségben, illetve a Szárazföldi haderőn belül.
- ismerje a NATO híradó és informatikai szervezeteit és azok működési rendjét.
- rendelkezzen ismeretekkel a híradás részterületein.
- kísérje figyelemmel a híradó technikai eszközök fejlődését.
- legyen tisztába híradó forgalmazás szabályaival, illetve a NATO híradó forgalmazási rendszabályainak és terminológiájának alkalmazásában.
- ismerje a szakaszánál (rajánál) rendszeresített híradó technikai eszközöket, azok alkalmazási lehetőségeit, illetve főbb harcászati-technikai adatait.
- professzionálisan tudja kezelni a rendszeresített híradó technikai eszközt (híradó állomását).
- ismerje az érvényben lévő kiképzési szakutasítások tartalmát, a híradó alegységekre és híradó katonákra vonatkozó kiképzési norma feladatokat.
- tegyen eleget a részére előírt osztályos követelményeknek.
- rendelkezzen REH alapismeretekkel.
- ismerje a híradó állomásához, előírt okmányokat, azok vezetésének szabályait.
- ismerje a híradó állomások szolgálati személyeinek feladatát.
- ismerje a híradó állomások technikai kiszolgálásának szabályait.
- ismerje és tudja alkalmazni a híradó állomás álcázási szabályait.

Ismerje:

- azokat a legfontosabb tervek rendeltetését és felépítését, amelyek az alakulatok béke és háborús működéshez rendelkezésére állnak.
- század szintig azon terveket, amelyek, a készenlét fokozására, a riasztási rendszer a személyi állománynak visszahívásához, az eszközei kiegészítéséhez, a tartalékosaik mozgósításához, mindezek fogadásához, az áttelepüléshez szükségesek.
- a szakasz békeidős működéséhez szükséges dokumentumok felépítését, elemeit.
- a szakasz békeidős feladatai végrehajtásához szükséges dokumentumokat.
- ismerje a különféle feladatok végrehajtásához szükséges egyéni és kollektív felszereléseket és anyagokat, legyen képes ezen felszerelések készség szintű alkalmazására.

- a szakcsapatnál rendszeresített lőszer, rakéta anyagok rendeltetését, valamint a hajtó illetve kenőanyagok sajátosságait, használati jellemzőit.
- a nukleáris, biológiai és vegyi védelemmel ellátott járművek, létesítmények védelmi lehetőségeit és azok alkalmazását.
- az áttelepülésre történő felkészülés mozzanatait, a tevékenység rendjét.
- áttelepülés előkészítésének szabályait, a települési hellyel szemben támasztott követelményeket.
- az áttelepülés végrehajtásának rendjét, annak minden oldalú biztosítási mozzanatait.
- az előírt jelentések megtételének rendjét.
- az előljáró irányába történő jelentések megtételének szabályait, azok tartalmát.
- az információs biztonság rendszabályait és legyen képes azokat a mindennapi tevékenység során hatékonyan alkalmazni
- a centralizált és decentralizált vezetés és feladat végrehajtás gyakorlati, készség szintű végrehajtását szakasz szintig.

A Tiszthelyettes mint kiképző

Kiképzésen a katonai feladatok megismerését és megtanítását, tehát a harcolni tudásra való felkészítést értjük. A kiképzés harci alkalmazásra készít fel, ezért kivétel nélkül harcszerűnek kell lennie. Minden más szempont háttérbe szorul. Az kiképzőnek a valóságra történő felkészítéshez reális, élethű harc-helyzetre van szüksége, s azt be is kell állítania. El kell tudnia képzelni és be kell mutatnia, hogy rá és embereire bizonyos körülmények között mi vár. Neki nem elég, hogy a fegyverét és a különböző harceszközöket kiválóan kezeli és tökéletesen alkalmazkodik a különböző harci viszonyok között a terepen. Ezeket az ismereteket át is kell adnia az embereinek, mégpedig olyan fokon, hogy a feladat teljesítése mellett életben is maradjanak.

A katonák műhelye a terep. Ezért a kiképzőnek nagyon kell szeretnie a természetet. Sem hidegben, sem melegben, sem esőben, sem viharban nem szabad félnie. Tudnia kell alkalmazkodni a helyzethez, hasznosítani a maga számára még a rosszat is, és ezeket tudnia kell átadni. Az kiképzőnek meg kell győznie a katonáit (az újoncokat), hogy a természet nemcsak élettér, hanem a katonák számára egyben túlélési tér is.

Térjünk vissza a harcszerűséghez. Mindig érdekes, izgalmas egy valóságos helyzetet megközelítő harcszerű kiképzés. A harckiképzés elsősorban a tiszthelyettesek fő munkaterülete. Pontosabban éppen az ebben való kiváló jártasságuk miatt kaptak, kapnak a tiszthelyettesek

kitüntető meghívást a különböző ENSZ-békefenntartó kötelékekbe. Ott érvényesítették tudásukat és be is bizonyították, hogy tiszthelyetteseink milyen mesterei szakterületeiknek. Egyébként is csak tiszthelyettes megy a „tanulóival” ütközetbe. A polgári életben a tanár elhagyja a diákjait, a diák a továbbiakban magára marad. A tiszthelyettes az ütközetben, harcban is katonáival van és velük is marad. Ott aztán minden kiderül. Az alárendelt minden hibája közvetlenül hat a parancsnokra is. Ha egy harckocsivezető hibát követ el, a harckocsi parancsnok és az irányzó azonnal érzi a következményeket. A kiképzésnek az a foka, amely képessé teszi a katonát, a harcra – kevés. A katonának akarnia is kell harcolni. A tudás és a képesség közvetítése a kiképzés során nevelési célzatú is, a katonák szívére, lelkére való ráhatással operál. Itt, ebben a körben az kiképzőre különös felelősség hárul. Hosszú időn át csak a szakmai teljesítmény megkövetelése áll előttük követelményként. A raj, szakasz összekovácsolása érdekében egyidejűleg alakítani kell valamennyi katona erkölcsi-morális értékeit. Miután mindegyikkel harcolni is akar, nevelni kell a katonát, formálni kell a jellemét. A tipikus katonaeurénysre, mint a hűség, állhatatosság, engedelmesség, bátorság, hősiesség, bajtársiasság a hagyományos módon nem lehet kiképezni. Mindezt következetesen bele kell nevelni a katonába. Többek között ezek miatt is különbözik a katona, a tiszthelyettes a tisztviselőktől, a tanároktól vagy a szakmunkásoktól. Hiszen egyetlen tanárnak sem kell iskolai osztályával halálos veszedelem között védelmeznie egy völgyzárógátat vagy egy repülőteret, és egyetlen villanyszerelőnek sem kell munkája elvégzéséhez a bajtársiasság, hanem a legjobb esetben is csupán segítség. Azonban annak a sebesült katonának, aki egy aknamező túlsó szélén, magatehetetlenül fekszik, szüksége van elszánt, bátor katonatársai segítségére. Egy légvédelmi ágyú irányzójának szüksége van a bátorságra, neki tovább kell tüzelnie, jóllehet mindenki más fedezékbe futott. Egy páncéltörő ágyú töltőkezelője nem hátrálhat, nem adhatja meg magát, töltenie kell talán mindhalálig...

Ezekre a magas szintű katonaeurénysre a katonát (katonáját) az tiszthelyettes neveli. Ehhez a tiszthelyettesnek mindenkor példaképpé kell válnia. A tiszthelyettesnek mindig bizonyítania kell, hogy „helyén van a szíve”. Ő csak akkor eszik, ha már valamennyi embere megkapta az ételét. Ő csak akkor hajtja álomra a fejét, ha már valamennyi emberének megvan a helye a pihenésre. Nem általában „hozza rendbe a dolgokat”, hanem segít a társát kihúzni a sárból, vagy felvenni a gázálcot és mindig ott van, ahol kell. Csak az olyan

tiszthelyettesek vívják ki embereik rokonszenvét, hűségét, akik egyformán bánnak embereikkel, nem „privilegizált lovagok”, nem „fedezékben kussolók”, de nem is „rambók”. Ezért volt igaza Prinz Eugennak, amikor tisztjeitől azt követelte: „Előbb megnevelni, kiképezni a katonát, és csak aztán követelni.”

Felhasznált irodalom:

A Magyar Honvédség hivatásos és szerződéses állományú katonáinak jogállásáról szóló 2001. évi XCV. Törvény
A honvédem négy éve 2002-2006 kiadvány
United States Army Field Manual (FM21-75)
Szép Lászlóné- A szerződéses katonák felkészítésének pedagógiai kihívásai

Erik PÁNDI:

Outsourcing of communication services in the field of public administration

1. Trends of outsourcing

There are two trends in the governmental outsourcing (OS) market. According to one of them the main purpose of outsourcing is the improvement of efficiency¹²¹ without applying radical changes in the organisational and operational courses. In this case the subject includes short-term, minor assignments for well defined and limited tasks¹²². The European governmental OS market is presently featured by these contract types.

The other approach intends to reach extensive and transparent governmental reforms and reorganisation by the long-term outsourcing of certain operational fields and activities. On this level of the OS activity the outsourcing of business process services¹²³ is more characteristic in contrast to the outsourcing of information-technology infrastructure and business solutions. For this reason the suppliers often struggle for the information-technology OS contracts,¹²⁴ as in the possession of such contract it is easier to get BPO agreements.

2. Trends in Europe

In the European civil OS practice¹²⁵ special emphasize is laid on contracts based on the connection between the private and state sphere. 2003 was the peak of governmental OS activity¹²⁶ in Europe, when there was considerable increase in the OS market portion of the civil sphere. In this year, 44 % of the information-technology OS contracts were concluded in the civil sphere; in the second half of 2004 the number of governmental and other civil service OS contracts has reached the level¹²⁷ of the OS activity of financial and insurance companies.

The number of OS contracts concluded in the civil sphere has been still increasing. The value of governmental contracts increased¹²⁸ by 78 % in 2004, that has definitely contributed to the 37 % increase in the total OS market.¹²⁹

¹²¹ cost cuts and quality improvement

¹²² contracting out

¹²³ BPO: business process outsourcing

¹²⁴ ITO

¹²⁵ mainly following the Great-Britain example

¹²⁶ due to these contracts a certain governmental function or action and the related responsibility are transferred to an outside party, however, the owner of the territory and the primary party in charge remains the state itself

¹²⁷ based on the data of the Forrester Research

¹²⁸ based on the analysis of the Datamonitor and Everest Group

¹²⁹ from 118,9 billion USD to 163 billion USD

Beside the quantity indicators, the volume, complexity and duration of the contracts have been also rising. The pulling force of the governmental OS activity is still in the increased governmental and civil administration information-technology investments,¹³⁰ however, the efforts made for the improvement of the quality and efficiency of governmental operation and civil services are taking more and more important part.

Great-Britain is beyond doubt the first in the OS gradation in Europe, both in quantity and quality. The British civil service OS market has increased by 228 % since 2000.¹³¹ The background of the British trend is partly ensured by the long-term centrally urged co-operation¹³² between the private and governmental sphere, based on the mutual sharing of risks. The essence of the British PPP-model is that the private sphere is involved in public tasks in a way, that the state gives into private hand not only the execution of the task, but also creating the method and conditions of supply; furthermore the investment itself too from financing to management.¹³³

Although the exclusively positive results of such co-operation are firmly questioned in Europe, PPP projects still play main role in the civil service OS practice. PPP projects show slow development in Europe,¹³⁴ the reason for that are the absence of European, central guidance and rules, furthermore the deficient knowledge of the member countries. In most of the EU member states academic planning is taken over by the period of action and similar development in volume to the British is expected in many countries in the near future.

Pursuant to recent observations the arguments for governmental resource outsourcing are supported now by the improvement of services and the idea of the availability of outside professional skills before cost saving. The duration of contracts is rather medium-term, three years in general.

3. Social effects of contracting out the resources

There is still significant interior opposition to the outsourcing practice in general, mainly due to data protection and other safety reasons, furthermore due to the unclear future of civil servants affected by outsourcing. The outsourcing of production and services is also encumbered by public anxiety for losing work and for the social price of globalisation. The rate of outsourcing can be hardly determined by figures. According to the EMCC

¹³⁰ the electronic governmental developments simultaneously require and generate the more complex information technology improvements

¹³¹ based on the analysis of Kable Ltd.

¹³² PPP: public/private partnership

¹³³ healthcare, traffic, education, etc.

¹³⁴ based on the analysis of Pricewaterhouse-Coopers of 2004

/European Monitoring Centre of Changes/¹³⁵ data since 2002 relocation and re-organisation into another EU member state or into a third country amounted to 7 %, while the outsourcing of resources¹³⁶ amounted only to 1,5 %. During the same period almost 8 % of the termination of work-places was caused by outsourcing¹³⁷, including replacing,¹³⁸ which is 5 %, and resource-outsourcing, that is 3 %.

Deep analysis of the outsourcing of resources can only show, what the announcement of deprivation and the presentation of negative economic effects really mean. The information-technology branch is often taken as an example for outsourcing services. In the territory of software development India possesses almost 70 % of the market share, however the information-technology and related services¹³⁹ still mean net work creating branches, that had created in the EU 175 thousand new workplaces between 1995-2002. According to the figures it seems, that outsourcing as a whole has created more workplaces, than it had abolished. At the same time the fluctuation of labour power has risen, that deepens the feeling of the doubtfulness of workplaces anyway. The latter feature of outsourcing shows at the same time, that much more attention shall be given to this phenomenon and adequate policy has to be developed for handling on each level from the company to the regional level, on the level of the individual countries and that of the EU as well.

Pursuant to the recommendation of the European Committee the agreement among the various interest groups is the key to the elaboration and application of an integrated strategy on the EU level. The directive on grouped cut-back and the directive on European operational boards both emphasize the right of employees, according to which in case of changes they have to be properly informed and consulted. The European operational boards have already confirmed their useful participation, as upon outsourcing they made the dialogue between the employees and the management easier. The EU plays an important part in inspiring the companies for undertaking social responsibility and assists the exchange of proper practices in Europe. The adoption of the voluntary code of conduct¹⁴⁰ seems to be such business decision, that can be advantageous for both the employees and the local community.

¹³⁵ EMCC

¹³⁶ rendering company services by a sub-contractor

¹³⁷ offshoring

¹³⁸ relocation

¹³⁹ which include hardware- and software counselling, and service, data processing and information-technology related maintenance

¹⁴⁰ in the framework of Corporate Social Responsibility initiations

4. Future trends

While in the last few years the advancement of OS in large enterprises and in the government had been significant, in the near future the global outtasking¹⁴¹ of individual business processes or that of some integrated company tasks¹⁴² are expected to increase more dynamically.

Another characteristic feature is nowadays, that beside the big multinational companies with international networks middle-sized companies are trying to allocate resources more frequently. The outsourcing of certain business activities and services plays significant role in the improvement of company efficiency and cutting operational costs. During the outsourcing of resources the companies do not essentially own the information infrastructure. Technological improvement becomes determinatively cost-based, this fact can result in the optimum utilization of available company resources. Based on this idea the state sector applies the outsourcing of certain activities in more and more developed countries. Examples for this phenomenon could be Great-Britain and the United States, where the entire outsourcing of partial tasks of a state organisation also occurs.

According to the international industrial experience civil administration does not have such field, which market participants could not enter. Almost 5-7 % of civil administration tasks are executed by outside companies in Great-Britain, the volume of out-organised tasks is expected to double within five years.

5. Summary

The outsourcing of resources in the information-technology sector of the Hungarian civil sphere has become a daily practice. International trends show, that the outsourcing of big supplying systems is now actual, that can arise in Hungary during the setting up of the Centre of Electronic Civil Services next year, as in the field of electronic government the Government intends to concentrate state resources of such degree and type serving functional activity, for which there was not any precedent earlier. In connection with the establishment of the Centre of Electronic Civil Services the outsourcing of functional territories becomes a strategic plan, that will be executed in the following years. We can only hope, that the conclusion of the OS contract really results in the cutting of costs and the improvement of quality beside the human alteration of application conditions.

¹⁴¹ outtasking

¹⁴² e.g.: improvement of information-technology systems closely connected to operation

Attila Takács

The status of the electronic civil service nowadays

1. The receiving eService

At the initiation of the Organic European Information Field in the action plan of 2010 the European Union determined as the one of the most important task the foundation of the information society that gives qualitative civil service. The conceptions of the receiving eService take the directives of the user into consideration more then in the past. These conceptions try to establish the leak of the social interest with the help of thematic Union forums came into existence in the course of local projects while these try to stop the factors that make difficult the social receiving with telehouses and other projects that help to acquire the information literacy.

The people can make use of on average 40 % of the services of the public offices in the EU the way of electrical. The new 15 member states of the EU are in about 10 % lower level than the other member states. In Hungary at the end of 2005 20 administrative procedures are available while the number of the downloadable form is about 200. Hungary now is an average country in the EU with the 18% range of eService. Analysis¹⁴³ shows that in spite of the low general usage of internet the large scale of the practice of eServices can be the correct way for the new member states. This can drive the people who don't use the internet towards the usage of the ICT equipment and new investments that connect with ICT. About the half of the population have the right attitude to eService. And the 40% of the people who know the eServices plane to try these services in the future.

The strategic decision-makers, the members of the civil service help everybody to use the online services. They start new supportive services for the open Hungarian society. By means of these services the possibility of the trying is available for everybody. Further development¹⁴⁴ established that there is a close connection between the tying of the online services and the satisfaction with these services or rather expansion of the claim. The utilization of these possibility further strengthen the consolidation of the receiving, the client centralized electronic civil service.

2. The civil service and the competitiveness

The information and communication technologies in large measure give a boost to the economy and the employment after all in the European Union the quarter of the increase of the GDP while 40% of productivity of the increase

¹⁴³ BME-UNESCO Information Society and Trend Researcher Centre and the INFONIA Foundation: eService – Years Report 2005.

¹⁴⁴ GKIE.NET: Self-governing survey, 2004.

can be attributed to the using of the ICT equipment. The governments become participant who can influence competitiveness by mean of development of eService while the civil service also must be competitive to the serve the competitiveness of the economy and society with the efficient function. The competitiveness supposes much rather a flexible, to able to respond to changes quickly, to able to satisfy claim of the users.

The importance and the dimension of the civil service basically influences the increase of the economy after all in 2003 in the 15 states of EU on the average 49% of the GDP was used by the civil services. This means that the civil service one of the largest customers in many European countries. The states can save the 5 % of cost wit the using of eServices therefore the spreading of these services is very important for every EU member states. The developing of the competitive government is very significant in the old Europe in the interest of required reduce of social expenses and unchanging economic development. In addition to idea of creation of the citizen centered civil services the promoting of competitiveness is standing in the centre of brand-new Union political thinking in connection with eServices.

As purpose the increase of efficiency, reduction of the costs of administration and approbation of the required changes in the establishments are formulated. In the connection with stimulating of the economy was formulated that recognition that the civil service can contribute to strengthen of increasing influence of productivity of information and communication equipment in three possible fields:

- a) investment to the ICT equipment,
- b) stimulation of production,
- c) usage.

With the help of ICT equipment the modernization of the civil services can't leave untouched the number of the employee. 17% of the employee in the whole Europe worked in the civil services while this rate in the USA is 16% and in Japan only 9%. In János Vadasz former government commissioner's¹⁴⁵ opinion that nowadays for 200.000 less people work in the civil service than in 1988 did in Hungary. But it is not so simple because in the power sphere the number of the employee is increased with 150.000. The number of the workers in the public institution is decreased with 300.000 in the last 16 years so compared these two quantities we can state that the supply of increasing task was solved first of all with the increasing of the employees and not with the rationalization of the processes on the servicing side. The most im-

¹⁴⁵ he was a government commissioner delegated to reorganize the structure of the civil service till 2005.

portant advantages for the citizens and for the businessmen are the quickness, quality and the flexibility in connection with eServices but unfortunately these features are not typical of mammoth enterprises like the civil services.

3. Existing problems, directions of development

A public opinion poll was completed by the European committee last year gives evidence of requiring of popularization of administrative possibilities to spreading of eServices. The services must be formed that it can be reachable and usable for everybody.

Nowadays the most difficult problem is the leak of the interconnection between active systems and complexity of the administrative availability. Enhancement of the communicational channels (mobile, digital TV) that use for contact can strengthen the attendance of the citizens. It is necessary to lay stress on the services connect to the public procurement, mobility of the citizens, the social insurance and the free flood of manpower in the period until 2010.

Since November of 2005 in Hungary the act CXL of 2004 makes availability that the costumers don't have to commute between bureaus in that case if they are in a sort of state or self-governing data base. In this case they are not obliged to collect data that are in other registers somewhere in the data bases of the authorities. In addition to this law the Costumer's Gate was also initiated last year that assures citizens and organizations of online availability of the administration after a single identification and authorization.

In Hungary the function of development were artificially separated in the local government and the central government. The informational integration between the administrative authorities and mission is not solved. The training of information science is defective. The most important thing for the most of the local governments is the obtaining and the keeping of the base infrastructure (suitable computers) and the leak of the good-quality internet connections. Therefore perhaps it is not surprising that only the 8 % of the local government is possessed written information technological strategy. Last year more than 40 developments were in the area of eService. Most of these were realized from EU assistance. But the on-line availability of these services is in the early stage. The most frequent on-line services in the local governments are registration of the changes of address, administration of the certificate of the authorities and permissions, the public libraries.

4. The functions of the governmental and defensive IT systems in the widening of the civil service

In the third part¹⁴⁶ of the development of the governmental telecommunication (after 9th January 2004) there are the possibilities to organize the unified governmental IT system in accordance with earlier idea of the strategy. This system can advance efficiently the governmental work and strengthening of the character of the supplier. By the act LV of 2006, about the list of the ministries in Hungarian Republic, and by the 144/2006 governmental decree, about the immediate changes in the leading of IT tasks, newer, more forceful centralization processes started that significantly affect the position and the function of the private networks in the future. If the control and the maintenance are in only one hand¹⁴⁷, it become possible to keep back the parallelism in the development and to realize the Union and national programs connected to electronic government. By means of integration¹⁴⁸ the number of the private telecommunication networks can be optimized that was formulated as the strategic idea previously.

5. Summary

The possibility of further development of cooperation according to the Union governing principle of communication systems of governmental and defensive sphere closely relates to the system of national electronic civil service (eService) and its state of development as network infrastructure serving eService and higher-degree integration of other private networks are expected next years.

Bibliography:

- [1] Baja, Ferenc: Reform a kormányzati informatikában, Írások az Internet és a média világáról 2002., Média Hungária Könyvek 4., Budapest, ISSN 1587-3846, pages 171-180, 2000
- [2] eEurope 2005: An information society for all (An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions), Commission of the European Communities, Brussels, 28. 5. 2002., COM (2002) 263 final, http://www.ihm.hu/tarsadalom/strategia/eeurope2005_en.pdf
- [3] Illyés, Mihály: Információtechnológia és telekommunikáció (ICT), Piacgazdaság Alapítvány, Budapest, ISSN 1586-9180, 2002.

¹⁴⁶ the evolutionary parts are established by Erik Pándi PhD

¹⁴⁷ Prime Minister's Office

¹⁴⁸ 2118/2006 governmental decree

- [4] Pándi, Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi, katonai és közigazgatási kommunikációs rendszerek megszervezésére és irányítására, PhD dissertation, Zrínyi Miklós National Defence University, Budapest, 2005
- [5] Dr. Tózsá István: m – Government, Magyar Közigazgatás, Vol 53/9, Budapest, ISSN 0865 736 X, pages 561-563, 2003

Kis Lajos mk. százados:

A vezetési pont hírközpontok modernizálása, avagy optikai eszközök a vezetési ponton

Napjainkra a vezetési pont hírközpontokban alkalmazott híradó állomások rendkívül elavultak, de az ország gazdasági helyzete nem teszi lehetővé az azonnali cserét. Véleményem szerint megfontolás tárgyát képezheti, hogy a rendelkezésre álló modernebb eszközökkel és kisebb anyagi ráfordítással modernizálhatók a jelenleg alkalmazott eszközök.

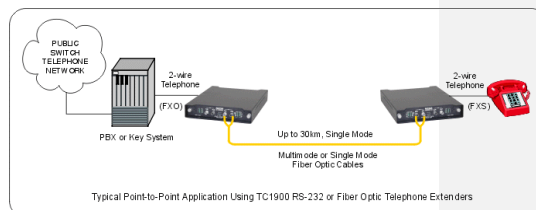
Elképzelésem szerint a jelenleg rendszerben álló és használt K-1 III M/G típusú távbeszélő központ állomások modernizálása történhet egy hasonló kapacitású elektronikus központtal (lásd.: a korábban nagy tömegben alkalmazott Samsung, Panasonic és Alcatel központok), mely meggyorsítja a távbeszélő forgalmat a vezetési ponton belül és abból kilépve. Szabványos hívószámokat alkalmazhatunk, a kezelői beavatkozás nem szükséges, a hívásoknál a kapcsolatok létesítésének ideje lerövidül, proirítások állíthatók be és sorolhatnám mindazon előnyt, melyet ezek a központok szolgáltatni képesek.

Természetesen a vezetékes vonalakat el kell juttatni a felhasználókhoz, amelyek nem a távbeszélő központ közvetlen közelében vannak. Ez a távolság akár 50-100-150 m is lehet (a terep adta lehetőségek és egyéb rendszabályok figyelembe vételével). Mondjuk ki, hogy a rendelkezésre álló elosztó kábelek nagy része nem képes kiszolgálni az igényeket, illetve a könnyűvezetékek és végberendezések sem képesek ezt maradéktalanul biztosítani. Megoldás lehet olyan átviteli eljárások alkalmazása, eszközök beszerzése, melyek „hasznoló”¹⁴⁹ kommunikációs háttérrel biztosítanak a felhasználók részére, mint „békében”. Az ún. POTS (Plain Old Telefon Service¹⁵⁰) eszközök alkalmazása jelentheti a megoldást.

Elképzelésem szerint a távbeszélő központba olyan optikai modemeket és/illetve multiplexereket kellene beépíteni, amelyek képesek a hagyományos analóg és a digitális vonalakat egy optikai érpárba/kábelbe átalakítani, illetve multiplexálni. Például:

¹⁴⁹ A „hasznoló” kommunikációs háttér alatt azt értem, hogy a szolgáltatások és azok minősége megközelíti a Magyar Honvédség Állandó Telepítésű Hírendszere által biztosítottat.

¹⁵⁰ <http://alpha.ttt.bme.hu/meresek/adslref.htm> - hagyományos telefonszolgáltatás.



1. ábra 2 huzalos áramkör továbbítása optikai kábelben

Forrás: http://www.arcelect.com/Fiber_Phone_and_RS-232_Extenders.htm



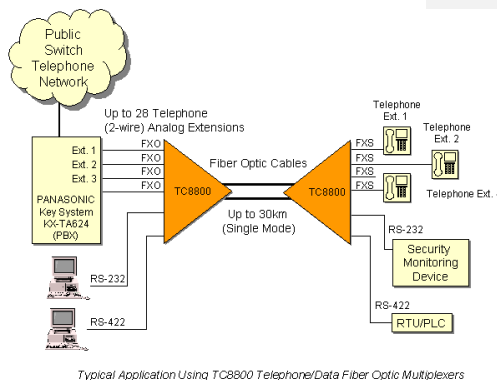
TC1900 Telephone to RS-232 or Fiber Extender (Shown with Telephone Set)

2. ábra TC1900

Forrás: http://www.arcelect.com/Fiber_Phone_and_RS-232_Extenders.htm

Ez a megoldás 1 db 2 huzalos áramkör nagytávolságú átvitelére alkalmas. Alkalmazási terület lehet nagyobb távolságra elkülönült mellékek (EÁP¹⁵¹, őrhelyek, egyedi - más helytől távoli végpont, stb. részére).

A következő megoldás, amikor több áramkör átvitelére van szükség egy optikai kábelben:



2. ábra több áramkör átvitele

Forrás: http://www.arcelect.com/ARC_fiber_optic_multiplexer_channel_bank.htm

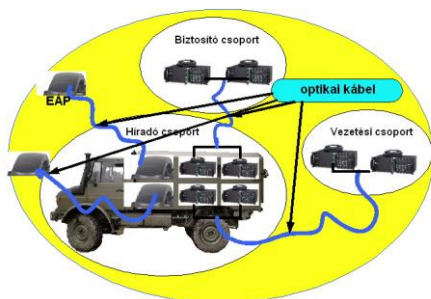
¹⁵¹ EÁP – Ellenőrző-Áteresztő Pont



3. ábra TC8800

Forrás: http://www.arcelect.com/ARC_fiber_optic_multiplexer_channel_bank.htm

E megvalósítási lehetőség alkalmas lehet a vezetési pont hírközpont (mint a vezetési pont része – híradó csoport) és a vezetési csoport (harcvezető központ, parancsnoki csoport, törzs csoport) közötti közvetlen vezetékes (optikai) összeköttetés megvalósítására.



4. ábra A híradó csoport és a vezetési csoport optikai kábellel való összeköttetése

Forrás: Saját

A példaként feltüntetett eszköz maximálisan 28 analóg kétvezetékes áramkört (vagy RS-232, RS-422) képes továbbítani egy optikai kábelen (minimum két optikai szál) maximálisan 30 km távolságra egymódusú optikai szál alkalmazásával, de átvitelre többmódusú optikai szál is alkalmazható. Azaz két ilyen kapacitású berendezés teljes mértékben ki kell hogy szolgálja a vezetési csoport kommunikációs igényeit. Természetesen fent említett megvalósítási lehetőségek csupán kiragadottak a fellelhető lehetőségek közül. Nem katonai, hanem hagyományos „polgári” célra kifejlesztett eszközökről van szó, azonban ezek szinte minden paraméterben megfelelnek a katonai elvárásoknak (páratartalom, hőmérséklet, mechanikai paraméterek, stb.). A berendezések közötti fizikai átviteli közegről is ejtsünk néhány szót. A kifejezetten katonai célra kifejlesztett optikai szálak és kábelek fizikai jellemzői alkalmassá teszik

a tábori körülmények közötti alkalmazásra (hő, szakítószilárdság, minimális hajlítási sugár, mechanikai szilárdság), melyek a későbbiekben rendszeresítésre kerülő korszerű rendszerekhez is alkalmazhatóak, tehát beszerzésük és rendszeresítésük nem „kidobott pénz”.

A fent alkalmazott eszközök, kábelek a következő előnyökkel rendelkezhetnek:

- A rövidebb telepítési idő megnövelné a hírközpont mobilitását, hiszen a több érpár helyett csak egy optikai kábel telepítése szükséges;
- Az optikai kábelek jól alkalmazhatóak az OTH¹⁵²-n biztosított lecsatlakozásokra;
- A felhasznált eszközök biztosítanak a rejtettséget;
- Az optikai kábelben történő összeköttetések egyfajta információvédelmet biztosítanak¹⁵³;
- Az optikai kábelek nem zavarhatóak és nem léphet fel kölcsönös zavarás sem;
- Üzemeltetési paraméterei széles tartományban mozoghatnak, ezért probléma nélkül alkalmazhatóak tábori körülmények között (üzemeltetési hőmérséklet: -10 °C-tól +50°, páratartalom 95%);

Hátrány lehet:

- az eszközök, kábelek beszerzésén kívül a beépítési költség;
- az interoperabilitás és kompatibilitás kialakítása más rendszerekkel, eszközökkel plusz költség;
- az állomány kiképzése.

Rövid írásomban szerettem volna a felhívni figyelmet arra a lehetőségre, hogy elavult rendszereinket fokozatosan is lehet modernizálni, ezáltal az állomány megszokja és elsajátítja a modern technológiák használatát. A felhasználók (parancsnokok és törzsek) olyan munkakörülmények között dolgozhatnak, mint máskor, békében.

Felhasznált irodalom:

- http://www.arcelect.com/ARC_fiber_optic_multiplexer_channel_bank.htm
- http://www.arcelect.com/Fiber_Phone_and_RS-232_Extenders.htm
- <http://www.tccomm.com/>
- <http://litelink.com/products/tlpx-1001.htm>
- <http://www.brugg.com/>

¹⁵² OTH – Országos Távközlő Hálózat

¹⁵³ Az optikai végberendezések az optikai kábelek paramétereinek „online” figyelésével, azok változásaira való reagálással (riasztás, kikapcsolás) biztosítják a lehallgatás elleni védelmet.

Kerti András mk. őrnagy:

A vezetés és a hírendszer kapcsolata

Az általam látogatott híradással, kommunikációval foglalkozó továbbképzéseken, és konferenciákon, miközben a színvonalasabbnál színvonalasabb előadásokat hallgattam, az a fajta hiányérzet alakult ki bennem, hogy az egyébként szakmailag jól felkészült előadók elfelejtik, hogy a híradás szolgáltatás. Szolgáltatás, mégpedig a katonai vezetés érdekében végzett szolgáltatás. Cikkemben megpróbálom feltárni, hogy a szakmai körökben már jó ideje előrevetített fejlődés milyen hatással lehet, magára a vezetés rendszerére, különös tekintettel a tábori hírendszerre.

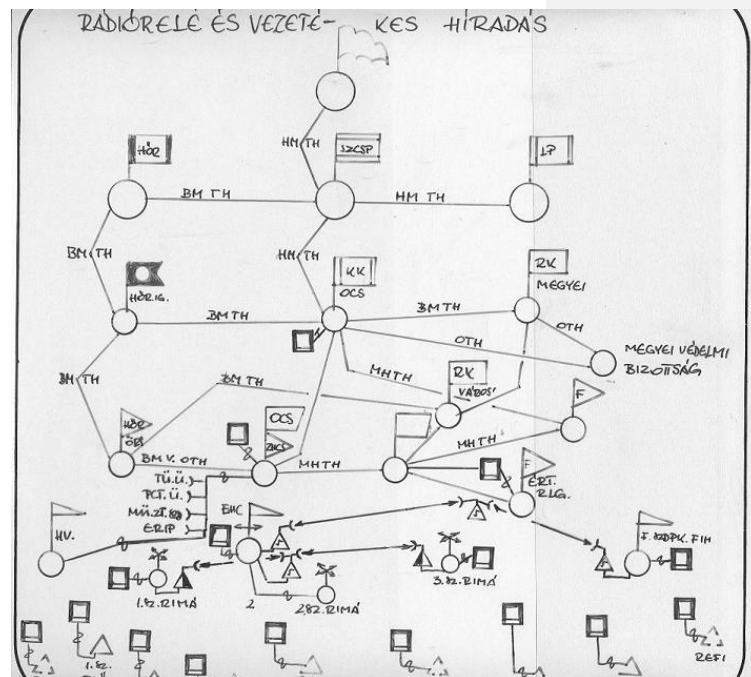
A katonai híradás fejlődése

Ahhoz hogy a nem túl távoli jövőre megfelelő következtetéseket tudjunk levonni át kell tekintenünk a katonai híradóhálózatok fejlődését. Természetes ez a téma olyan nagy, hogy akár egy nagy doktori disszertáció anyagát is kiölthetné, ezért itt csak az általam fontosnak tartott jellemzőkre térek ki, amelyeket lényegesnek tartottam

Lineáris hírendszer: Hírközpontok közvetlen összekötése.

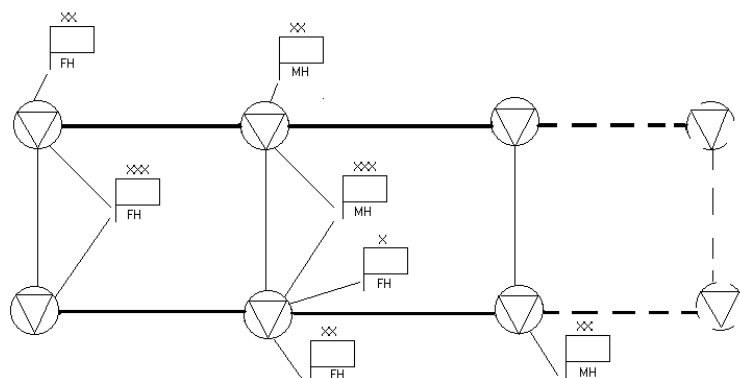
A katonai híradásban a vezetékes eszközök megjelenésével a különböző végpontokat vagy közvetlenül pont-pont összeköttetésekkel valósították meg, amely összeköttetések e főirányokba, illetve a különösen fontos tevékenységet végző szervezetek irányába volt jellemző, illetve központokba gyűjtötték őket, ahonnan a központ kezelő személyzete osztotta szét a csatornákat az igényeknek megfelelően. A rendszer egyértelmű hátrányai voltak: egy (vagy akár több) szervezet hírendszerből való kikapcsolásához, elég volt azt a hírközpontot likvidálni, amelyhez csatlakozott (csatlakoztak), a harc dinamikájának megfelelően, a vezetési pontok hírközpontjait, a csatlakozó vezetékes vonalakat naponta akár többször át kellett telepíteni. Mindkét problémára bizonyos megoldást kínált a rádió eszközökkel megvalósított, hírhálózat, valamint ha az idő engedte, egy szervezetet több hírközponthoz (kiszolgáló hírközpont, országos hálózat) is csatlakoztattak. Ezáltal lehetőség nyílt a kerülő utak biztosítására. Az alábbi ábrán egy a 90-s évekből származó ZMKA-n oktatásra került fólia szkennelt változata látható, amely a lineáris hírendszert mutatja be.¹⁵⁴

¹⁵⁴ A fóliát Dr. Sándor Miklós nyá. ezredes bocsátotta rendelkezésemre az archívumból.



294

elégséges volta miatt alakult így. A 2. számú ábrán, egy ilyen hírendszér sémáját láthatjuk.



7. ábra

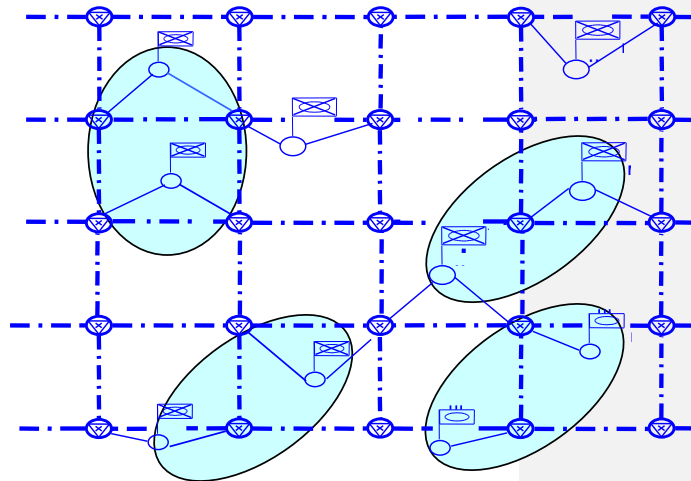
A NATO kommunikációs rendszerek a hadműveleti területen egy rácsrendszerű, területlefedő hálózat kialakítására törekednek, megfelelő hírközpont-sűrűséggel. Ez azt jelenti, hogy a domborzat és a kommunikációs igények figyelembe vételével a csomópontokat a hadműveleti területen egymástól légvonalban 15-25 km-re helyezik el. Majd azokat a szomszédos csomópontokkal összekötik, így alakítva ki egy komplex kommunikációs hálózatot (3. ábra). Ez a rendszer nem feltételez tengelyeket, mint a tábori alaphírhálózat, mert a hadműveleti terület uralgó magaslati pontjain elhelyezett csomópontok azonos szolgáltatásokat képesek nyújtani mindenki részére a vezetés érdekében. Ezek a csomópontok azonos képességekkel rendelkeznek, így a rendszer minden pontján képes fogadni a különböző vezetési pontok hírközpontjainak csatlakozását a harcászati köteléktől egészen a vezérkarig.¹⁵⁵

A területlefedő rácsrendszerek közös jellemzője az automatikus útvonal keresési rendszer. A kommunikációs hálózatok a hívott fél keresését, az összeköttetés felépítését és létesítését automatikusan valósítják meg, az előre meghatározott fizikai, vagy logikai útvonal kiválasztásnak megfelelően.¹⁵⁶

¹⁵⁵ Rajnai Zoltán mk őrnagy: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetősége egyes NATO tagországok kommunikációs rendszereinek tükrében (Doktori értekezés) ZMNE 2001

¹⁵⁶ A polgári életben a mobil telefonok hálózathoz való kapcsolódásában hasonló elveket követnek, de a szakirodalomban általában a csomópontok által elérhető területeket szokták ábrázolni, de ha a csomópontokat összekötő csatornákat jelölnénk, megkapnánk a területlefedő hírendszert. Ezért neveztem az alcímben ezeket a rendszereket „cellás”-nak.

Tudomásom szerint ez a elv még jelenleg is működik. Kezdetben az analóg csomóponti összeköttetéseket felváltották a digitális átvitel technikai csatornák, majd egyre inkább alkalmasak lettek, adat továbbításra is és fejlődésileg egyre jobban közelítenek, közelítettek az általam következő szintnek tartott megoldáshoz.



8. ábra

Itt szeretném megemlíteni, hogy a két rendszer között nem csak a technikai lehetőségek miatt volt különbség, hanem a különböző hadikultúrák szervezési elvei miatt is. Mert addig, amíg a Varsó Szerződés országai a mozgás centrikus hadikultúra elkötelezett hívei voltak, addig Európa nyugati felén az anyag centrikus hadikultúra dívott és dívik. Az előbbinél a fő hangsúly a támadásra tevődött, míg az utóbbinál a hadászati védelem, az ellenség kifárasztása a stratégiai cél. A mozgás centrikus hadikultúrában a hadműveleteket fő és mellék hadműveletekre osztották, és így érthető, hogy a fontosabb irányokban nagyobb harccselekményekkel számoltak, és ezeknek a várható információ áramlása is nagyobb volt. Az anyag centrikus hadikultúra által tervezett hadműveletekben nincsenek kiemelt fontosságú irányok, mindegyiket egyforma fontosnak tartják, így elméletileg az információ áramlás valószínűsíthető nagysága is megegyező a harctér minden irányában.

Harcászati internet

A már meglévő technikai lehetőségek és kommunikációs rendszerek szervezési elvei előrevetítik egy következő, minőségileg új szervezésű rendszer lehetőségeit, amelyekkel a nálunk technikailag fejlettebb országok már különböző gyakorlatokon illetve hadműveletekben tesztelnek. Ez az új rendszer földrajzi topológiájában nem különbözik a cellás rendszerektől, a változás az információk továbbításának kivitelezésében van.

Az IP/TCP alapú hálózatok technikai kivitelezéséről, tapasztalatairól ten-gernyi az irodalom és ezt nem kívánom tovább szaporítani, inkább szervezési oldalról próbálom meg megközelíteni az általa hozott változásokat.

Ebben a rendszerben a berendezéseket, eszközöket véleményem szerint4 csoportba oszthatjuk:

Beviteli és megjelenítő eszközök.

A helyi hálózat eszközei.

A nagytávolságú átvitelt megvalósító eszközök

Valamint inkább logikai, mint valóságos eszközök a szoftverek.

A Csoportok között lehet átfedés, és mindegyik csoportot tovább lehet osztani. Az első csoportba tartoznak a jelenlegi un. Híradó végberendezések (telefon, fax, kamera), a különböző szenzorok, érzékelők stb... Ebben a csoportba sorolom a személyi használatú számítógépet is nem csak azért mert ezekkel különböző információkat (billeentyűzet, adathordozók) lehet bevinni, hanem mert bizonyos feldolgozott információkat továbbíthatnak a hálózat felé. Igaz, egy személyi számítógép akár egy kisebb szerver is lehet és itt máris eljutottunk a második csoporthoz.

A helyi hálózat eszközei: Véleményem szerint ebbe csoportba tartoznak a különféle szerverek, switchek, routerek, hubok. Ide tartozónak gondolom a központi rendeltetésű háttértárolókat és minden egyéb olyan eszközt amelyeket manapság mint a számítógépes hálózat elemeiként ismerünk.

A harmadik csoport megalkotásánál azokra az eszközökre gondoltam, amelyek a nagytávolságú összeköttetéseket biztosítják, és különböző hálózatokat kötnék össze. Ebben az esetben is lehet átfedés mert ki mondja meg mi az a nagy távolságú és hol végződik egy kiterjedtebb helyi hálózat és hol kezdődik a másik? Ezek lehetnek nagytávolságú optikai kábelek, mikrohullámú eszközök, műholdas összeköttetések.

A negyedik csoportba sorolt szoftverek alkotják a rendszer lelkét melyek nélkül, az egész rendszerre költött javak csak kidobott pénzt jelentenének, ezért az árúk is ehhez mérhető. A szoftvereket célszerű két különböző alcsoportba sorolni:

A hálózatot üzemeltető vezérlő és felügyeleti-;
Egyéb felhasználói szoftverek.

Az utóbbihoz tartoznak az „egyszerűbb” irodai szoftvereken a különböző döntés-előkészítő, analízist végrehajtó programokon keresztül a 3D-s megjelenítő szoftvereken át minden olyan szoftverek amelyek végső soron a parancsnokot segítik a munkájában (a törzsén keresztül). Alkalmazásuknak három dolog szabhat határt: a parancsnok fantáziája, a szoftverfejlesztők tehetsége, és a rendelkezésre álló pénz.

Az előbbi csoportba tartozó szoftverek nem csak a rendszer felépítésekor játszanak szerepet, hanem annak alkalmazásakor, mivel az egész rendszer szoftveres úton vezérelhető és különféle szervezési elveknek tehet eleget a felhasználás során. Ilyen lehet például: prioritások biztosítása valamely meghatározott csatornán, információk, belépési lehetőségek letiltása, módosítása, és virtuális „magán” hálózatok létrehozása, a parancsnok igényei szerint.

Az új infokommunikációs rendszer hatása vezetési rendszerre

Mielőtt létrehoznunk egy internet jellegű infokommunikációs rendszert, vizsgáljuk meg a csapatok vezetése érdekében meg kell vizsgálnunk milyen problémákat vethet fel ez a vezetés tekintetében és milyen problémákat vethet fel.

Ahhoz hogy ezt meg tudjuk tenni, vizsgáljuk meg a Magyar Honvédség jelenlegi vezetési rendszerét. A jelenlegi vezetési rendszerben a vezetés szintet tudunk megkülönböztetni:

A csapatok, végrehajtó szervezetek közvetlen vezetése, ide tartoznak az önálló alegységek, ezredek, dandárok vezetése;

A középvezetési szint a Szárazföldi Parancsnokság, a Légierő Parancsnokság, Összhaderőnemi Logisztikai Támogató Parancsnokság, Híradó és Informatikai Parancsnokság, Budapesti Helyőrség Parancsnokság, stb.

A katonai felső vezetési szint Honvéd Vezérkar és a Honvédelmi Minisztérium. A 4. ábrán látjuk ennek egy vázlatos sémáját.

formázott: Nincs

formázott: Betűtípus: Times New Roman, 12 pt

formázott: Betűtípus: Times New Roman, 12 pt, Nem Dőlt

formázott: Betűtípus: Times New Roman, 12 pt, Nem Dőlt

formázott: Betűtípus: Times New Roman, 12 pt, Nem Dőlt

formázott: Betűtípus: Times New Roman, 12 pt, Nem Dőlt

kításához szükséges e szakemberek közreműködése, mert ők ismerik a rendszer lehetőségeit a legjobban. És ez felvet egy másik dolgot: csak akkor tudnak jó javaslatokat adni a rendszer kialakításához, ha az infokommunikációs szakemberek jártasak az összefegyvernemi törzs munkájában is.

A mostanában szinte rendszeresen ismétlődő árvízi vészhelyzetekhez kapcsolódó katonai feladatok végrehajtásának tapasztalatai, bizonyos előrejelzésekre adnak lehetőséget. Ezekben a feladatokban a fő infokommunikációs eszköz a mobil telefon, illetve a honvédség zártcélú hálózata, amely rendelkezik a polgári mobiltelefon hálózatokhoz kapcsolódó szolgáltatással. Már ezeket az eszközöket használva is jelentősen megnőtt az információ áramlás sebessége a 10 évvel ezelőtti viszonyokhoz képest. A védelmi munkacsoportok sürgős kirendelésekor többször előfordult, hogy, a feladat végrehajtása előbb elkezdődött, mint a hivatalos ügyirat a végrehajtóhoz leérkezett. (Természetesen, az elrendelésre jogosult szóbeli engedélyével, illetve parancsára.) Az se ritka eset, hogy a felső szintről jövő intézkedések a középső szint operatív csoportjánál, csak átfejlécezésre, az aláírás kicserélésére korlátozódtak.

Ha ezeket a tapasztalatokat, kivetítjük más esetekre is és ezekből próbálunk meg következtetéseket levonni számomra két dolog következik:

A jelenlegi csak papír alapú parancs-utasítási rendszert át kell dolgozni a kornak megfelelő elektronikus ügyintézésre, amelyben a papír alapú rendszer minden előnye megmarad, a hátrányai kiküszöbölése mellett.

A jelenlegi struktúrában meglévő vezetési szinteket háromról kettőre lehet csökkenteni, és ezzel jelentős forrásokat (anyagi-, emberi-, és idő-) lehet megtakarítani.¹⁵⁷

Befejezés

A jelen dolgozatomban a híradórendszerek fejlődés történetének vázlatos áttekintése után megpróbáltam feltárni a jövő katonai infokommunikációs rendszerét szervezési oldalról.

Véleményem szerint a megjósolt (nem csak általam) rendszer egy hadügyi, hadelméleti „forradalmat” is kell hogy elindítson. Ennek folyamán meg kell változni a parancsnoki vezetési rendszernek, változnia kell a vezetési struktúrának a vezetésben dolgozó ügyintézők feladatrendszerének és felelősségi körének. Szintén változni kell a vezetési struktúrának is.

Felhasznált irodalom:

Haig Zsolt-Várhegyi István Hadviselés az információs hadszíntéren Budapest
Zrínyi kiadó 2005

¹⁵⁷ A jelenleg (2006. szeptember október) folyó átszervezési feladatok nem csökkentik a vezetési szintek számát csak a középvezetési szinteket vonják össze, és ez nem a már meglévő technikai lehetőségek kihasználása.

Dr Szép József: A NATO új kezdeményezése: a hálózat nyújtotta képesség Új Honvédségi szemle

Rajnai Zoltán mk őrnagy: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetősége egyes NATO tagországok kommunikációs rendszereinek tükrében (Doktori értekezés) ZMNE 2001

Dr. Rajnai Zoltán mk. alezredes: A tábori hálózat felügyelet felépítése és funkciói Habilitációs eljárás, szakmai vita. 2006. szeptember 11. Budapest ZMNE

[Ly1] megjegyzést írt: A többi még meg kell keresni!!

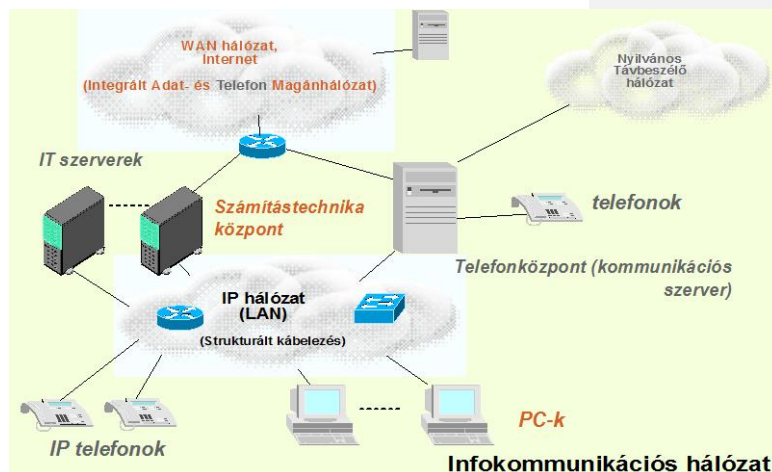
Rajnai József (SIEMENS):

Hogyan tovább? Útkeresés a Magyar Honvédség hírrendszerében

Tegyük fel néhány kérdést a jelenlegi 52 központból (49 Hicom 300H és 3 HiPath 4000) álló stacioner hírközlő hálózattal kapcsolatban: Készen van? Lehet még javítani? Megérett a modernizálásra? Hogyan tovább? Igyekszem ezekre a kérdésekre választ adni. Ki-ki döntse el saját szakterületének kommunikációs igényeit számba véve, hogy mi a válasz a feltett kérdésekre.

Az alábbi ábrán látható infokommunikációs infrastruktúra jellemző napjainkban.

Ez a modell viszonylag rövid és a legutóbbi tíz évben rohamosan felgyorsult fejlődés eredménye. Kezdetben az informatikai és a telefonhálózat a hozzájuk kapcsolódó szolgáltatásokkal két, szigorú határokkal elkülönített terület volt. A telephelyek közötti informatikai (adat) és telefonos (hang) kapcsolatokat kezdetben szintén párhuzamosan építették ki és a két rendszer között semmilyen átjárás nem volt. 6-8 évvel ezelőtt kezdett tömegesen elterjedni az a technológia, ami lehetővé tette két telephely telefonhálózatának összekapcsolását a – meglévő - informatikai adathálózaton keresztül; ezzel kialakultak egy integrált hang-adat WAN hálózat alapjai.



A további fejlődés eredményeképpen megjelentek olyan telefonközpontok, amelyek az informatikai hálózat részeként képesek –akár egy bármilyen másik szerver- üzemelni. Ezek a kommunikációs szerverek egyrészt megteremtik a kapcsolatot az informatikai hálózaton kívüli világgal (Nyilvános Távbeszélő

Hálózat, analóg fax készülékek és egyéb analóg készülékek), másrészt vezérlik az egységes multimédia hálózatra (LAN) kapcsolt telefonkészülékeket. A különálló hang- és adatkommunikációs hálózatok tehát teljesen egybeolvadtak egy közös infokommunikációs hálózattá.

A kommunikáció hatásköre, a hírközlő rendszerrel szemben támasztható és támasztandó elvárások

A hírközlő rendszer a fentiek szerinti megközelítésben az IT rendszer egyik alrendszere. A továbbiakban megnézzük, melyek ennek az alrendszernek a már ma is meglévő főbb jellemzői, amikre a jövőben is célszerű építkezni. Számba vesszük azokat az elvárásokat, amelyek teljesítésére a meglévő rendszer képes, illetve viszonylag alacsony költséggel képessé tehető, illetve adunk egy receptet arra, miként biztosítható, hogy a kialakított rendszer mindenkor a legmagasabb technológiai színvonalán álljon és működjön.

Megbízhatóság, rugalmasság, biztonság

A Siemens által megvalósított, és folyamatosan bővülő hírközlő rendszer magas szintű rendelkezésre állását egyrészt a kipróbált és többszörösen tartálékolt hardver és a hálózattírányításban alkalmazott redundanciák biztosítják. Másrészt a rendszer-architektúra csúcsán a felügyeleti központok (OHF, TOHF) a Siemens szakemberei által folyamatosan képzett rendszerfelügyelők révén egységes konfiguráció- hiba- és irányításmenedzsmenttel járulnak hozzá üzemeltetési oldalról ahhoz, hogy soha ne fordulhasson elő szolgáltatáskiesés. A rugalmasság a konfiguráció, a bővíthetőség, a szofisztikált hálózattírányítás, a végkészülékek típusának és azok egymáshoz képesti arányának, az interfészek számának és típusának tekintetében értendő. Mindezt a rendszer úgy biztosítja, hogy a módosításokkal járó költségek minimálisak. A biztonság egyrészt biztonságos adatkezelést jelent: központi menedzsmentet és adattárolást valósítottunk meg, így az egyes hírközlési csomópontokon nem nyerhető ki sem a Honvédség teljes felhasználói adatbázisa, sem pedig a teljes hálózat irányítására vonatkozó információk. Másrészt a (továbbfejlesztett, HiPath 4000) rendszer jelzés- és beszédtitkosítási eljárások használatát kínálja.

Jelzés-és beszédtitkosítási eljárások a HiPath 4000 rendszerben

A HiPath 4000 V3.0 hálózat CorNet IP végkészülékei között (IP telefonok) 128 bites kóddal SRTP AES titkosítást kínál a rendszer mind a jelzés, mind pedig a payload (besztédátvitel) számára. A titkosítás azokban a viszonylatokban alkalmazható, amelyek egymással az IP hálózaton keresztül kapcsolatban állnak (tehát nincs pl. ISDN hálózati szakasz a jelzés, vagy beszédútban).

Illeszkedés a meglévő rendszerekhez

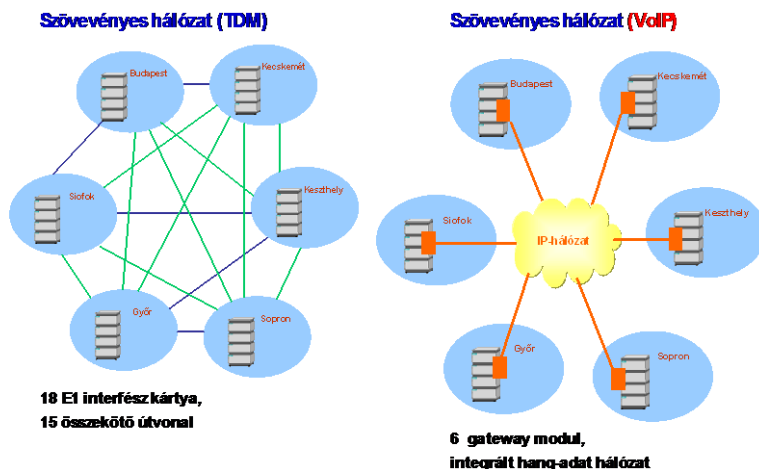
A rendszernek a meglévő analóg hálózába kellett úgy beépülni, hogy a kommunikáció folyamatosan zavartalan legyen és kapcsolatot kellett biztosítani a NATO hálózatokhoz (STANAG 5040 és Eurocom D1) is. Ezek analóg- és digitális MFC-R2 illetve E&M interfészekben valósulnak meg. Napjainkban természetesen az analóg kapcsolatok iránti igényt egyre inkább felváltja, illetve azzal párhuzamosan jelentkezik a digitális ISDN, esetenként az IP interfészen történő illesztés. Az előzőekben említett rugalmasság lehetővé teszi, hogy ezeket az igényeket gyorsan és költséghatékonyan tudjuk ebben a rendszerben kielégíteni.

Alkalmazkodás a mindenkori hálózati infrastruktúrához

A mai stacioner hírközlési hálózat alapvetően a mikrohullámú átviteli rendszer topológiáját követő egymással ISDN E1 interfészekben összekapcsolt Hicom 300H típusú kapcsolóközpontokból áll. Mindenhol, ahol erre lehetőség van, a biztonság növelése érdekében kihasználjuk a redundáns kapcsolati lehetőségeket és a központok fejlett hálózati technológiája automatikusan vált a használható útvonalra. A rerouting és route optimizing szolgáltatások biztosítják a teljes hálózat automatikus intelligens működését optimális sávszélesség kihasználás mellett.

Az új MPLS IT gerinchálózat kihasználásának lehetősége

Az Iroda-Automatizálási Projekt keretében szükségessé válik az átviteli rendszerek korszerűsítése. Az informatikai alkalmazások bevezetésével megnövekedett sávszélesség-igény kielégítése egyrészt a sávszélességek növelésével, másrészt a meglévők kihasználásának optimalizálásával érhető el. A HiPath 4000 kommunikációs szerver - mely a Hicom 300H IP IT hálózába illeszthető változata – a jelenleg alkalmazott Hicom 300H minden szolgáltatását és előnyét megtartva, egyszerűen beépíthető az új IP infrastruktúrába. A beépítés alapvető célja és előnye a sávszélesség optimális kihasználása, azaz két szomszédos csomópont között nem foglal le a rendszer állandó sávszélességet, miként az ISDN hálózati kapcsolatok esetében, hanem csak annyit, amennyit az éppen fennálló beszélgetések lebonyolítása indokol. Ezzel a módszerrel drasztikusan csökken a kapcsolatok létrehozásához szükséges fizikai interfészek száma, ugyanakkor a logikai kapcsolatokat nem változtatjuk, illetve azok minden további költség nélkül változtathatók, bővíthetők. Az alábbi két ábra a Hicom rendszerben alkalmazott fix sávszélességigényű ISDN, illetve a HiPath rendszerrel megvalósítható IP hálózati struktúrát mutatja.



Nyilvánvaló, hogy az előzőekben kifejtett előnyök csak a HiPath szervereknek az informatikai (hordozó)hálózatba történő integrálásával aknázhatók ki.

Erre fizikailag két lehetőség kínálkozik:

Az **egyik esetben** a telephelyeken (csomópontokon) lévő WAN routerbe építünk E1 interfészt és a Hicom 300H (vagy a HiPath 4000 amely a Hicom 300H-hoz hasonlóan továbbra is támogatja az E1-et) megfelelő E1 interfészét azzal kötjük össze. Figyelembe kell vennünk azt is, hogy a kommunikációs hálózat több viszonylatában nem 1, hanem 3, sőt 4 E1 interfészre is szükség van.

Erre a **másik esetben** nincs szükség, hisz a router rendelkezik a LAN oldalon IP (Ethernet) interfésszel, melyhez a HiPath 4000 közvetlenül csatlakoztatható.

Felmerül a kérdés, hogy melyik opciót célszerű alkalmazni?

Egyértelmű, hogy a másodikat, azaz a **HiPath 4000**-re frissített központokat azok IP interfészein közvetlenül csatlakoztassuk a routerre. Miért?

- **mert** mindent egybevetve **olcsóbb**, mint az első megoldás: lehetséges, hogy az E1 betétet működtetni képes WAN router és a benne elhelyezett E1 betét(ek) ára önmagában nem magasabb, mind egy adott Hicom --> HiPath upgrade ára, azonban egy ilyen megoldás viszonylag hosszú időre késleltetheti azt a bizonyos upgrade-et, ezáltal további hatékonyságnövelő és költségcsökkentő megoldások (ezeket a továbbiakban ismertetjük) bevezetésének gátjává válik, valamint a hírsziszter fejlesztését a jelenlegi szintre befagyasztja.

- mert **növeli a hálózat rendelkezésre állását** az első megoldáshoz képest, amely szükségtelenül növeli az alkalmazott hardver elemek számát és azok bonyolultságát, miáltal az üzemeltetési költségek is növekednek.

Hatékonyág, költségcsökkentés

A mai stacionáris hírközlő rendszer kielégíti a Magyar Honvédségnek a hírközlő rendszerrel szemben támasztott alapvető igényeit. A beszékkommunikáció megbízható, bizonyos speciális rendszereket mint a veszprémi és kecskeméti légiirányítás megfelelően integráltunk a kommunikációs rendszerbe. A hálózat megfelel speciális katonai és nemzetvédelmi előírásoknak, szabályzóknak is.

Napjainkban a Honvédség berkein belül is előtérbe kerültek az alcímben megfogalmazott fogalmak: Nem elég a beruházásnak kedvező árszinten megvalósulni, de fontos, hogy az **üzemeltetési költségek minél alacsonyabbak** legyenek, sőt az eddigiekhez képest lehetőleg **megtakarítást** is érjünk el az új eszközzel/rendszerrel. Ráadásul a Magyar Honvédségnek egyre csökkenő létszámmal kell egyre jobban működnie, betöltenie nem csekély hivatását: hazánk védelmét. Sokan nem is sejtik, milyen **hatékony segítséget** tud ehhez a kihíváshoz nyújtani a megfelelően kialakított, **modern kommunikációs rendszer**, melynek alapja, gerince a Hicom hírközlő rendszer képében ma rendelkezésre áll.

A meglévő Hicom rendszer az anyagi eszközök rendelkezésre állásának függvényében lépésről-lépésre alakítható HiPath 4000 rendszerré, melyben az IT rendszerekkel szoros együttműködésben már a kezdetektől biztosíthatók a hatékonyság növelésének és a költségek csökkentésének eszközei. Az alábbiakban ismertetünk néhányat ezekből a megoldásokból:

A kommunikációs költségek mérése és igazságos elosztása

A jól beállított díjszámláló rendszer lényege nem az, hogy korlátozzuk a telefonálási lehetőségeket, hanem hogy optimalizáljuk a telefonhasználatot. Azáltal, hogy a munkatársak tudatában vannak annak, hogy beszélgetéseik adatait rögzítik, ösztönösen jobban figyelnek arra, hogy csak a szükséges hívásokat bonyolítsák. A szigorú költségelosztási rendszerben már nem egy nagyszámból fizetik a telefonálás költségeit, hanem pontosan kimutatható, hogy melyik csoport (sőt azon belül egyes személyek) mennyit és hova telefonált - megszűnt a mindent elfedő anonymítás. Ez nem csak ahhoz vezet, hogy **csökkennek a telefonköltségek**, hanem a dolgozók – mivel csak a legfontosabb magánbeszélgetéseket engedhetik meg maguknak, azokat is rövidre fogják – több időt fordítanak a munkavégzésre is. A telefonköltségek pontosabb elosztásához, illetve korlátozások bevezetéséhez lehetőség van a PIN kódos illetve projekt kódos telefonálás bevezetésére is.

A mérés és elosztás központilag, az OHF rendszerben történik, ezzel biztosítva van “szolgáltatás szolgáltatásának” a hatékonysága is.

HiPath Xpressions üzenetkezelő rendszer

A hang- és faxposta többek között arra alkalmas, hogy ha a keresett személyt azonnal nem lehet elérni, „legalább” üzenet hagyható a számára, és amint módjában áll, válaszolni fog rá. Az alkalmazásnak van kiértékelés opciója ami annyit tesz, hogy a hang- vagy faxpostafiók tulajdonosa meghatározhatja, hogy a rendszer értesítse őt telefonon vagy pl. SMS-ben üzenet érkezésekor, miáltal az üzenethez való hozzájutás már **nem esetleges és igen gyorsan** megtörténhet. A rendszer megfelelő jogosultsággal VPN csatornán keresztül bárhol elérhető (a hálózaton kívülről is), az üzenetek elolvashatók.

A HiPath Xpressions minden típusú üzenetet (Hang, Fax, E-mail, SMS) egy közös felhasználói felületre integrál, például MS Exchange környezetben Outlook kliensre, és megteremti az egyes médiák között az átjárást (pl. fax-üzenetet e-mailben továbbíthat a lekérdezéskor, vagy e-mail üzenetet felolvas telefonba). A rendszer fax-posta szolgáltatásával rengeteg papír és dologi költség, valamint az egyedi faxok karbantartásának költsége is **megtakarítható**.

HiPath GSM Integráció

A HiPath GSM Integráció olyan megoldás, amely lehetővé teszi, hogy a Siemens HiPath rendszerének előfizetője az irodai mellékére érkező hívásokat tetszés szerint mobil készülékén fogadja. A GSM Integráció szolgáltatásai révén a Siemens HiPath rendszer képes úgy kezelni a külső (mobil)hálózati készüléket, mintha az közvetlenül a kommunikációs rendszerhez csatlakoztatott mellék lenne. Elegendő a keresett személy HiPath rendszeren belüli hívószámának ismerete. Aki ezt hívja, az párhuzamosan csörgeti a felhasználó mobil számát, vagy egy alternatív, előre definiált hívószámot. A mobil telefonon felvett hívás rögzíthető, tovább kapcsolható belső számra, a hívó tartásba helyezhető és új hívás kezdeményezhető, a tartásba helyezett hívó később visszavehető a tartásból. A rögzített beszélgetés automatikusan a felhasználó e-mail fiókjába (előre megadott címre) kerül. Ennek az alkalmazásnak a használatával jelentősen **növelhető** a fontos személyek **elérhetősége**, ezzel az intézkedések, mozgósítások gyorsasága, **hatékonysága javul**.

Távmunka

A **Távmunka** lehetősége adott a modern HiPath kommunikációs környezetben. A PC-vel és telefonnal (ami lehet a PC-n futó „szoftphone”) kialakított távmunkahelyet egy biztonságos csatornán (VPN, például ADSL szolgáltatón keresztül) összekapcsoljuk a központi infokommunikációs környezettel (HiPath és irodai alkalmazások). Az így kialakított munkahely minden tekintetben úgy viselkedik, mintha a központban lévő irodában lenne. Bárki lehet

távmunkás, akinek nem szükséges a napi munkája során a rendszeres személyes jelenlét a munkahelyen. Ezzel utazási és elhelyezési **költségek takaríthatók meg**, viszonylag csekély szolgáltatói díj ellenében.

HiPath Wireless LAN portfólió

Használata indokolt, ha az intézményen belül bárhol egyszerűen hozzáférhetőnek kell lenniük az erőforrások és az adatoknak, vagy amikor nagyon gyorsan, szinte órák alatt kell működőképes irodai környezetet létesíteni, vagy pl. műemlék épületek irodai használata során, amikor nincs lehetőség az épületben kábelezés kiépítésére. A WLAN (Wireless LAN) az IP forgalom szempontjából transzparens megoldás, ezért nem csak a klasszikus adatforgalom, hanem a multimédiás IP alkalmazások (hang, kép) ideális átviteli közege is. A HiPath WLAN portfólió komplett megoldás: lehetővé teszi a vállalaton belüli valódi mobilitás megvalósítását. A portfólió WLAN (mobil) telefonkészülékeket, WLAN hozzáférési pontokat és vezérlőegységeket kínál, kiváló management szoftverekkel és a tervezést és megvalósítást is magában foglaló, teljes körű támogatással. A teljes Honvédségi hálózatban bárhol biztosíthatók a szolgáltatásai az OHF-ben és TOHF-ben elhelyezett clusterban működő vezérlőegységekkel.

HiPath Easy programcsomag

Ez a CTI szolgáltatás-csomag olyan új innovatív szolgáltatásokat nyújt a kijelzővel rendelkező HiPath 4000 optipoint illetve optiClient felhasználói számára, amelyekkel munkavégzés **hatékonysága** jelentősen növelhető. A csomag többek között az alábbi modulokat kínálja:

- EasyMail

Az EasyMail segítségével Ön telefonkészüléke gombnyomására PC-jén új e-mail megírását kezdeményezheti, az éppen beszélgetésben lévő partner(ek) e-mail címével automatikusan megcímezve. (A levelezőablak előugrik.)

- EasyShare

Az EasyShare segítségével a telefonon egy gombnyomással Microsoft Netmeeting kapcsolatot létesíthet beszélgetőpartnerével, illetve a címtárban szereplő egyéb felhasználókkal is. Így például konferenciát kezdeményezhet egy dokumentum megbeszélésére, kamera használatával pedig egyetlen gombnyomásra video-kapcsolatba kerül a címzettel, tehát meglévő telefonbeszélgetését PC-je segítségével **video kapcsolattal** egészítheti ki.

Openscape

A Microsoft Windows 2003 .Net IM (Instant Messaging) szolgáltatás kommunikációs kiegészítő szoftvere a Siemens HiPath Openscape nevű alkalmazása, ami az IM szolgáltatást kiterjeszti a teljes kommunikációra, egy felületen jelenítve meg a munkatársak valamennyi elérhetőségét; összekap-

csolja a számítástechnikai- és a hang-kommunikációs rendszert és lehetőséget biztosít ez utóbbi szolgáltatásainak használatára.

A HiPath Openscape növeli az egyes dolgozók és a csapatok kommunikációjának hatékonyságát, mert a keresett személy(ek) elérhetőségét mutatja és ezért azonnal a megfelelő módon lehet próbálkozni a kapcsolatteremtéssel, másrészt a kapcsolatteremtéshez nem szükséges médiaváltás: azaz bármelyik elérési lehetőség esetén a PC használatos, mint média és felhasználói felület.

Meet-me konferencia rendszer

A HiPath 4000 alközpontok számára a sokrésztvevős (8-nál több) beszéd konferenciát a központ vezérlő c-PCI architektúrájába illeszkedő Meet-me conference Server (MMCS) biztosítja. A szerveren összesen 1000 konferencia szoba hozható létre maximálisan 30 résztvevővel. A konferencia szerver segítségével a konferencia résztvevői bárholnan bejelentkezhetnek a kívánt konferenciára a meghatározott időpontban. Az egyes Chat és konferencia szobákhoz különböző hozzáférési jogosultságok állíthatók be. A szerver központilag elhelyezhető.

Informális CallCenter

A Honvédség kötelékében elsősorban a Hadkiegészítő Parancsnokságokon bevezethető szolgáltatás. Olyan CallCenter is kialakítható, mely az intézményben elszórtan helyet foglaló (sőt akár távmunkában dolgozó) különböző területekért felelős dolgozókat tömöríti a technika segítségével egy közös elektronikus ügyfélszolgálati (jellegű) rendszerbe. A HiPath Procenter Agile rentábilisan működtethető már 4-5 tagú ügyintézői/ügyfélszolgálati csoportokban is. Az Agile egy nagyon hatásos „fegyverrel” rendelkezik: a jelenléteszleléssel. Ebben az esetben ez azt jelenti, hogy minden callcenter ügyintéző képernyőjén láthatók azoknak a személyeknek az elérési lehetőségei, akik a saját területükön, mint konzultációs, vagy döntéshozó partnerek szóba jöhetnek. Ez nagyban növeli az ilyen munkakörökben dolgozók hatékonyságát.

A hálózat fejlesztésének javasolt módszertana

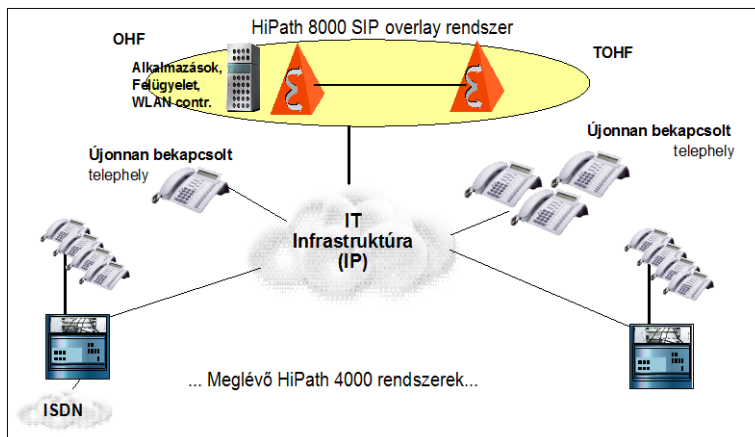
Az a jó gazda, aki nem hagyja, hogy háza az enyészeté legyen – javíttatja, fejleszt, bővíti. Tán nem volt pénz a napkollektorokra az építéskor, de tudjuk, ha lassan is megtérül, ezért most beruházunk rá. A fürdőszoba is új berendezést kap, a központi fűtést felújítjuk és vegyes tüzelésű kazánt szerzünk be. Mind-mind azért, hogy a házunk értékét megőrizzük, hogy az adott időben - *anyagi helyzetünk keretein belül* – a legmagasabb technikai színvonalon elégeithessük ki igényeinket. Ritkább eset, mert többre kerül és finanszírozási szempontból sem kedvező, hogy a lerobbant, elavult épületből új, modern házba költözünk.

A katonai fejlesztésekről ma is köztudott, hogy gazdagabb országokban előbbre járnak a civil technológiáknál. Érvényes ez minden szakterületre. Mi ezt még nem engedhetjük meg magunknak, de törekedhetünk arra, hogy a jó gazdához hasonló módszerrel legalább a civil szféra state-of-the-art (a jelenleg elérhető legmagasabb technikai színvonal) technológiáját alkalmazzuk.

Tegyük ezt úgy, hogy miközben fitten tartjuk jelenlegi rendszerünket – azaz az aktuális szükségleteknek megfelelően bővítjük, frissítjük, hatékony alkalmazásokkal egészítjük ki, kidolgozzuk azt a koncepciót, amelynek mentén a majdani aktuális hírközlő rendszert átemeljük egy filozófiájában más, az alábbi ábrán látható úgynevezett hosted rendszerbe. Természetesen lehet e körültkintő előkészítő munka eredménye, hogy a Magyar Honvédség számára nem megfelelő a most felvázolt architektúra, de nem tehetjük meg, hogy figyelmen kívül hagyjuk mint lehetséges megoldást a továbbfejlesztésre. Az infokommunikációs szakma elemzései ugyanis azt mutatják, hogy az ilyen rendszereké a jövő és 2012-15-re jelentős szerepet játszanak majd a világ magánhálózati kommunikációjában.

Meglátásunk szerint ezt a cél-architektúrát legelőbb 3-5 év távlatában érdemes elérni. Ennek a szolgáltatói szemléletű rendszernek a középpontjában az ábrán overlay rendszerként megnevezett két, egymástól fizikailag távoli clusterben üzemelő HiPath 8000 softswitch áll. A HiPath 8000 vezérlők robosztus, redundáns IBM szervereken, Resilient Telco Platform middleware-en futó Linux alkalmazások. A HiPath 8000-re regisztráló SIP előfizetők száma több 10,000 lehet. Ebben a rendszerben a meglévő HiPath 4000 rendszerek gateway funkciót töltenek be a Nyilvános Távbeszélő Hálózat, a megmaradó analóg telefonok, faxok és egyes kommunikációs alkalmazások felé. A hálózatban előforduló minden további kommunikációs igényt praktikusán a HiPath 8000 fog kiszolgálni, így az újonnan bekapcsolt telephelyek (IP) készülékei mind a HiPath 8000-re regisztrálnak.

A HiPath 4000 központokat idővel új generációs célhardverek (túlélő Gateway-k), a rendszertelefonokat pedig a HiPath 8000-re regisztráló IP készülékek fogják – lépcsőről-lépésre kiváltani. Az átalakítás idején a HiPath 4000 hálózathoz kapcsolódó központi kommunikációs alkalmazásokat a HiPath 8000-hez migráljuk.



A HiPath 8000 rendszer előnye a nyílt szabványokon alapuló alkalmazások, egyszerű, az informatikai rendszerbe simuló architektúra, a beruházási és fenntartási költségek viszonylagosan alacsony szintje – magas szolgáltatási színvonallal párosuló rendkívül gazdaságos üzemeltetés.

Bízunk benne, hogy eljutunk közösen ahhoz a ponthoz, hogy alkalmazását komolyan megfontoljuk.

Fregan Beatrix :

L'avancée des perspectives européennes

En matière de défense, trois pays, la France, la Grande-Bretagne et l'Allemagne, ont une position dominante en Europe et sont capables d'influer sur le cours des événements. Les années passées ont montré le rôle moteur que peuvent jouer ces trois pays lorsqu'ils agissent de concert. Pour des raisons historiques, par leur poids économique et industriel, et grâce à leur image sur la scène internationale, ils ont également un rôle déterminant pour la réalisation de grands programmes d'armement. Ces trois pays sont les seuls à posséder sur le continent européen une base industrielle de défense autonome, performante et couvrant tout le spectre des technologies. Ces trois Etats ne sont certes pas tous les trois indispensables pour la réalisation d'un grand projet, mais actuellement aucun programme d'intérêt stratégique militaire ne pourra vraiment voir le jour si deux de ces pays en sont absents. En résumé, pour l'instant, et sans doute encore pour la prochaine décennie, en matière de défense, rien de réellement stratégique ne pourra se faire en l'absence de la Grande-Bretagne, de l'Allemagne ou de la France.

Outre la capacité financière, ces trois pays sont les seuls à pouvoir donner un caractère structurant à un programme dépassant ainsi le seul aspect de la performance technologique.

L'environnement économique

Des progrès considérables ont été réalisés au cours des années passées mais le facteur politique transatlantique s'ajoute aux aspects économiques. En dépit des menaces que font peser la prolifération des armes de destruction massive et le terrorisme, notamment depuis les événements du Onze Septembre, le constat actuel montre un environnement peu favorable au lancement et au développement de grands programmes militaires d'intérêt stratégique.

Compte tenu de leur coût considérable et des contraintes budgétaires, les grands programmes d'intérêt stratégique militaires ne peuvent plus actuellement être conduits dans un seul cadre national. Les grands pays européens sont par ailleurs confrontés à une situation économique difficile, réduisant les marges de manœuvre des gouvernements et des entreprises. Parfois interdépendantes, les origines de ces difficultés sont principalement les suivantes :

- une faible croissance au cours des années 2001 à 2003, à la limite d'une récession pendant quelques mois ;
- une compétition économique accrue sous l'effet de la mondialisation ;

- une absence de marge budgétaire liée essentiellement à une augmentation considérable des charges des Etats, notamment la charge de la dette, le coût de la protection sociale et la poursuite de grands programmes déjà engagés (Rafale, Eurofighter, A400M, VBCI, NH90, TIGRE), et d'un autre côté, à une diminution des ressources lorsque les gouvernements cherchent à réduire les impôts et les taxes;
- la perte du levier de l'instrument monétaire depuis l'entrée en vigueur de l'Union économique et monétaire et de l'Euro en 1999¹⁵⁸, la Banque centrale européenne étant indépendante du pouvoir politique des membres de la zone Euro.

En matière de programme d'armement, l'inventaire de l'action européenne recouvre trois types d'existant :

- des Traités européens où les aspects de défense ne sont pas totalement absents, notamment avec le Traité de Maastricht par exemple ;
- des déclarations politiques sous l'impulsion déterminante de la Grande-Bretagne et de la France, comme à l'occasion des sommets à Saint-Malo en 1998 et au Touquet en 2003 ;
- des structures de coopération hors du cadre de l'Union européenne, comme l'Organisation conjointe de coopération en matière d'armement (OCCAR)¹⁵⁹ et la Lettre d'Intention, *Letter of Intent* (LoI)¹⁶⁰.

Le Traité de Maastricht¹⁶¹ spécifie que les questions de défense font partie du second pilier consacré à la Politique étrangère et de sécurité commune (PESC). La possibilité de création d'une Agence européenne de l'armement figure déjà en annexe de ce traité.

¹⁵⁸ L'Euro a été créé le 1^{er} janvier 1999 avec la fixation des taux de change et avec la mise en œuvre d'une politique monétaire unique sous la responsabilité de la BCE. Il est entré en service le 1^{er} janvier 2002.

¹⁵⁹ Créée en novembre 1996 par l'Allemagne, la France, l'Italie et le Royaume-Uni et pourvue d'une personnalité juridique depuis janvier 2001, l'OCCAR vise à favoriser une collaboration plus concrète et efficace dans les programmes d'armement. Elle a pour mission de coordonner, conduire et faire exécuter les programmes que les Etats fondateurs décident de lui confier et de lancer des activités communes de préparation de l'avenir.

¹⁶⁰ Signée à Farnborough en juillet 1998 par l'Allemagne, la France, l'Italie, l'Espagne, la Suède et le Royaume-Uni, et suivie en 2000 d'un Accord-cadre juridiquement contraignant, la LoI vise à faciliter les restructurations de l'industrie de défense en Europe, au travers d'une harmonisation des réglementations nationales.

¹⁶¹ Traité sur l'Union européenne signé à Maastricht en février 1992 et entré en vigueur en novembre 1993.

Le sommet de Saint-Malo¹⁶² peut être considéré comme le véritable point de départ de l'Europe de la Défense. Le 4 février 2003 au Touquet, la Déclaration sur le renforcement de la coopération en matière de sécurité et de défense propose des « *initiatives pour moderniser et développer les capacités de l'Europe en matière de défense et de sécurité* ». Ces propositions relativement innovantes concernent :

- des moyens avec la définition d' « *objectifs quantitatifs (indicateurs pertinents de dépenses de défense), et qualitatifs (disponibilité, efficacité militaire, déployabilité, interopérabilité et soutenabilité des forces)* » ;
- un instrument avec la mise en place au sein de l'Union européenne d'une « *agence inter-gouvernementale de développement et d'acquisition des capacités de défense* » dont l'objectif serait de « *promouvoir une approche globale de développement des capacités par tous les Etats membres de l'UE* ».

L'objectif de l'OCCAR et de la LoI est de rendre plus efficace la gestion des programmes d'armement réalisés en coopération. Ces existants montrent déjà l'importance de la volonté des Européens pour progresser vers un cadre plus favorable aux programmes d'intérêt stratégique militaire.

Aujourd'hui une véritable perspective d'évolution se dessine au niveau politique. Les Européens ont récemment franchi une étape importante en mettant sur la table, une vision et un instrument. En effet, deux éléments pourront être à l'origine d'une évolution potentiellement considérable :

- l'émergence d'une vision stratégique commune sous l'impulsion de Javier Solana¹⁶³, haut représentant de l'Union européenne pour la Politique étrangère et de sécurité commune (PESC) dans le document intitulé « *Une Europe sûre dans un monde meilleur* »¹⁶⁴ ;
- la création de l'Agence européenne de l'armement qui a vu le jour au cours de l'année 2004.

Jusqu'au mois de juin 2003, à l'opposé d'autres domaines, la défense était peu présente au niveau du Conseil européen. Lors du Conseil de Thessalonique, Javier Solana a esquissé ce qui pourrait constituer la vision stratégique de l'Union européenne qui « *permettra à l'Union européenne de mieux lutter contre les menaces et les défis mondiaux et de tirer parti des*

¹⁶² Déclaration franco-britannique lors du Sommet de Saint-Malo le 4 décembre 1998 reconnaissant que « *l'Union européenne doit avoir la capacité de lancer des actions autonomes, soutenue par des forces militaires crédibles, avec les moyens de les mettre en place afin de répondre à d'éventuelles crises internationales* ».

¹⁶³ Javier Solana a assuré les fonctions de Secrétaire général de l'OTAN du mois de décembre 1995 au mois d'octobre 1999 avant d'être nommé à sa fonction actuelle le 18 octobre 1999.

¹⁶⁴ Le Conseil européen de Bruxelles du 12 décembre 2003 a adopté ce document qui constitue la « *stratégie européenne de sécurité* ».

possibilités qui se présenteront »¹⁶⁵. Ce document donne aux Etats membres une nouvelle dimension à leur ambition stratégique qui était jusqu'alors réduite à la gestion des crises.

Considérant la sécurité comme une condition nécessaire du développement, Javier Solana distingue cinq grandes menaces dont la conjugaison peut être à l'origine d'un décuplement de leur ampleur : le terrorisme, la prolifération des armes de destruction massive, les conflits régionaux, la déliquescence des Etats et la criminalité organisée.

Par ailleurs, les objectifs de l'Agence sont les suivants :

- le premier, opérationnel et à court terme, développer les capacités de défense dans le domaine de la gestion des crises ;
- le second, plus ambitieux et à moyen terme, promouvoir et renforcer la coopération européenne en matière d'armement, renforcer la base technologique et industrielle européenne en matière de défense et créer un marché européen concurrentiel des équipements de défense.

Vers une Politique commune d'armement

En matière d'équipements de défense, la Commission européenne¹⁶⁶ a fait des propositions pour contribuer à la réalisation d'objectifs plus ambitieux. Elles concernent notamment la restructuration et la consolidation de l'industrie, le renforcement de sa compétitivité, et l'établissement d'un marché européen des équipements de défense. Toutefois, il faut continuer de développer ces propositions si l'on souhaite traiter la question dans sa globalité.

Une volonté politique pourrait trouver sa traduction au sein d'une « Politique commune d'armement » (PCA) approuvée par le Conseil européen et mise en œuvre sous l'égide de la Commission européenne. Une telle politique pourrait notamment tirer bénéfice des apports et des acquis de l'expérience des politiques communautaires existant déjà. Elle pourrait également tirer des enseignements de leurs faiblesses et de leurs difficultés. Cette politique commune d'armement pourrait permettre l'émergence au niveau européen de programmes militaires.

¹⁶⁵ Conclusion de la Présidence – Bruxelles, le 12 décembre 2003

¹⁶⁶ Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions « Défense européenne – Questions liées à l'industrie et au marché – Vers une politique de l'Union européenne en matière d'équipements de défense », Bruxelles, le 11 mars 2003.



LOWE GOM

Hajózni márpedig kell... aggódni nem muszáj!

A T-Systems új menedzselte szolgáltatásai - menedzselte LAN-, hang- és biztonsági szolgáltatások - biztosítják a háttérét annak, hogy Ön azzal foglalkozzon, amivel valóban szükséges. A hálózati és üzleti szempontból kritikus alkalmazások üzemeltetésével és felügyeletével kapcsolatos gondokat levesszük az Ön válláról. Adja át magát a fontos feladatoknak, és összpontosítson a kormányzásra! Hajózni így érdemes! T-Systems menedzselte szolgáltatások. www.t-systems.hu

Business flexibility

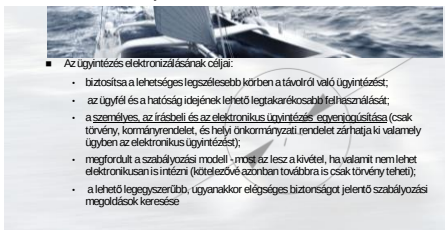
Fazekas Béla (T-Systems):

Közigazgatási szolgáltatások a Magyar Telekom Nyrt-től



KET – lépés a szolgáltató állam felé

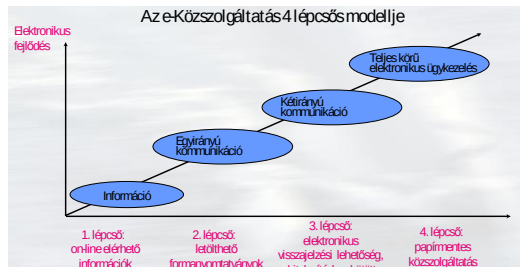
A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXLI. törvény



Az e-kormányzás jövőképe



Elektronikus közszolgáltatás fejlődése



...T...Systems...

2006. október
3. oldal

Elektronikus ügyintézés példái



...T...Systems...

2006. október
4. oldal

Az elektronikus ügyintézés megvalósítása

■ Elektronikus tájékoztató szolgáltatás: A közigazgatási szervek tájékoztatási nyújtanak elektronikus formában (kötelesek):

- A szervezetről, elérhetőségeiről, ügymenetről, ügyintézők neveiről és más, általuk fontosnak ítélt információiról - ennek kiterjesztése, részletesebb szabályozása várható az elektronikus információszabadságról szóló törvényben
- A vonatkozó jogszabályokról, ügyintézési határidőkről, az elektronikus ügyintézés lehetőségéről, módjairól, a beadvány kitöltésének módjáról, az eljárás illeték vagy más díj megfizetésének módjáról
- az elektronikus ügyintézésben résztvevő szervezetnek biztosítania kell, hogy az ügyekkel kapcsolatos információk naprakészek, hitelesek és az interneten keresztül is elérhetőek legyenek

■ Elektronikus ügyintézés:

- az Ügyfélkapun keresztül,
- az EKG infrastruktúráján,
- az intézmények háttérrendszereire épülő alkalmazásokkal

■ A személyes adatok védelme az ügyintézés folyamatában biztosított

...T...Systems...

2006. október
5. oldal

Az elektronikus ügyintézés



- Központi Elektronikus Szolgáltató Rendszer biztosítja, hogy
 - az ügyfélnek ne kelljen minden eljárás formai szabályait, eljárásait külön-külön megtanulni
 - ne kelljen minden szervezetnek önállóan az azonosítás, hitelesítés infrastruktúrát létrehozni
 - az ügyfél a számára nyitott ügyfélkapun keresztül intézheti ügyeit, kommunikálhat a hatóságokkal (elektronikus aláírás nélkül, jelszavával azonosítva szűkebb ügykörben, elektronikus aláírással szélesebb körben)
 - a központi rendszer biztosítja hogy a hatóság tudja, kivel áll kapcsolatban, de az ügyfél ne kényszerüljön szükségtelen eljárás (azonosítás) lépésekre, kiegészítő szolgáltatások - pl. biztonságos tárolás, időpecsét
 - a központi rendszer működéséért a Kormány által kijelölt kormányzati szerv (MEH-EKG) felelős - 1053/2004 Korm. határozat

... T ... Systems

2006. október
6. oldal

A központi rendszer funkciói



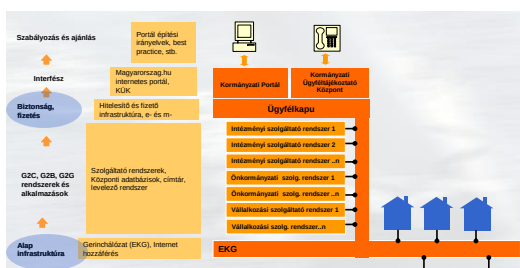
- A 184/2004 (VI. 3.) Korm. rendelet szerint a Központi Elektronikus Szolgáltató Rendszer magába foglalja az alábbiakat:
 - Elektronikus Kormányzati Gerinchálózat (EKG)
 - Kormányzati Portál (www.magyarorszag.hu)
 - Szolgáltatások és ügyintézési lehetőségek a Kormányzati Portálon (támogatására – Kormányzati Ügyféltájékoztató Központ (KÜK))
 - Ügyfélkapu létesítési lehetőség biztosítása
- A Ket. (2004. évi CXII. törvény) szerint az elektronikus ügyintézés lehetőségét – ha az ügyfélnek nincs elektronikus aláírása – a központi rendszer biztosítja
- A 1044/2005. (V. 11.) Korm. határozat alapján felügyeletét és üzemeltetését a Miniszterelnöki Hivatal biztosítja

A központi rendszer az E-kormányzati Közmű „motorja”

... T ... Systems

2006. október
7. oldal

A központi rendszer és a Közmű



... T ... Systems

2006. október
8. oldal

Elektronikus Kormányzati Gerinchálózat szolgáltatás

- Szolgáltatási szerződés: 2005. április 25.
- A szerződés tárgya: a Műszaki és Szolgáltatási Specifikációban meghatározott szolgáltatásoknak nyújtása, így különösen:
 - Országos gerinchálózati szolgáltatás nyújtása a Felhasználó telephelyén biztosított csatlakozási felülettel;
 - Budapesti optikai összeköttetések nyújtása a Felhasználó telephelyén biztosított csatlakozási felülettel;
 - Az EKG Internet szolgáltatásának biztosítása;
 - VoIP alapú hangszolgáltatás elindítása és folyamatos szolgáltatása 900 telephely vonatkozásában
 - Hálózathibabiztonsági feltételek garantálása, hálózati felügyelet biztosítása;
 - A Szerződés keretében a Szolgáltató általi fejlesztések megvalósítása, és az ennek keretében létrejövő új szolgáltatások működtetése a Műszaki és Szolgáltatási Specifikáció szerinti Emeltszintű szolgáltatások fejezetének figyelembe vételével.

...T...Systems

2005. október
5. 09:08

A szerződés időtartama

- A Szerződés a szerződés hatályba lépésétől 2009. december 31-ig terjedő időszakra jött létre
- Szolgáltató az eszközöket 2009. december 31-én a Magyar Állam tulajdonába adja át.

...T...Systems

2005. október
31. 09:08

A felhasználó intézmények előnyei az EKG-ra csatlakozás esetén

- Az EKG igénybevételével sávszélesség bővítés hajtható végre
- Ingyenes telefonálási lehetőség a Kormányzati hálózaton belül. (Felhasználó valamint a Felhasználói csoporton belül)
- A felcsatlakozáshoz CE routert biztosítunk
- A meglévő PSTN kapcsolatok egy része lemondható (~40-50%)
- A jelenlegi eszközpark a lehetőségek szerint felhasználható
- A díjmegtakarítások emeltszintű szolgáltatások igénybevételére fordíthatók
- Egykapus üzemeltetés és hibabejelentés, magas fokú üzembiztonság

...T...Systems

2005. október
11. 09:08

Szolgáltatási keretszerződés

■ Szolgáltatási keretszerződés megkötése 2005. december 19.

■ A Keretszerződéshez a felhasználó intézmények egyszerű Megrendeléssel csatlakozhatnak.

■ Tárgya, szolgáltatások: „A jelen szerződés tárgya az EKG központi szolgáltatásainak MEGRENDELŐK számára történő biztosítása, melyek a következők:

- emelt szintű integrált adatszolgáltatás;
- VoIP alapú hangszolgáltatás;
- központi címtár;
- központi levelező rendszer;
- időbélyeg szolgáltatás;
- informatikai biztonsági és védelmi szolgáltatások;
- videokonferencia központi szolgáltatás;
- elektronikus adatszere szolgáltatás (EDI);
- távmunka szolgáltatás központi elemei;
- e-learning szolgáltatás központi elemei.”



... T ... Systems

2005. október 12. 9:58

Az EKG hálózat műszaki jellemzői:



■ A hálózat alapja DWDM technológia

■ 6 db Gigabit Ethernet gyűrűvel kerül megvalósításra

■ A gerinchálózat topológiája gyűrűs védelmet biztosít.

■ MT és az EKG csomópontokat független optikai nyomvonalak kötik össze.

■ A hálózat megbízhatóságát duplikált központ biztosítja



... T ... Systems

2005. október 12. 9:58

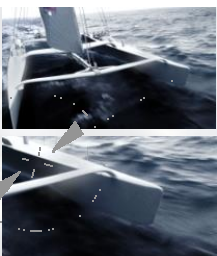
Az EKG hálózat műszaki jellemzői:

■ Tartalékolás

■ Az Intézményi aggregált forgalmát 34 és 155 Mbps összeköttetésen keresztül adjuk át az EKG hálózatba

■ Esetleges csomóponti kieséskor az EKG felé az Intézményi összeköttetést a MT az MLLN hálózaton keresztül biztosítja

■ Az Intézményi átkapcsolásokat a MT 30 percen belül elvégzi



... T ... Systems

2005. október 12. 9:58

Az EKG hálózat műszaki jellemzői:

■ Internet kapcsolat

- Az EKG hálózat, megbízható duplikált Internet összeköttetést biztosít
- Az Internet kapcsolaton a Kopint-Datorg megerősített tűzfal védelmet nyújt
- Nemzetközi Internet forgalmat dedikált nemzetközi összeköttetések biztosítják
- Közvetlen kapcsolat az EU Testa hálózatához



... T Systems

2006. május
15. 08:58

Az EKG pályázat célkitűzéseinek megvalósulása



- Forrásbevonás
 - 2009. végéig +12 milliárd Ft
- Költségsökkentés
 - a korábbi üzemeltetési költség csökkentése
 - a csatlakozó intézményeknél a hálózati üzemeltetési költségek megszűnnek
 - a hangszolgáltatás (VoIP) forgalma 2006. január 1-től az EKG-n belül ingyenes
 - az értéknövelt szolgáltatásoknál kedvezményes díjak
- Rácsatlakozás felgyorsítása
 - eddig erőforráshiány miatt lassabban haladt
- Új szolgáltatások indítása
 - a szerződés szerint fokozatosan indulnak
- Szolgáltatási képesség dinamikus javítása
 - az üzemeltetés-biztonság növelése (mission critical szint elérése)
 - a hálózat funkcionális bővítése

... T Systems

2006. május
16. 08:58

Jövőkép

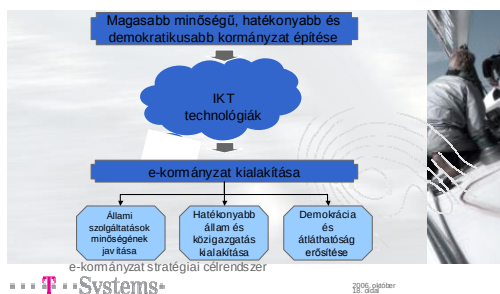


- Magas minőségű, egységes hálózat
- Szolgáltatások körének jelentős bővülése (pl. VoIP, kormányzati levelező rendszer, címtár, videokonferencia stb.)
- EU adatbázisok, szolgáltatások elérésének biztosítása biztonságos hálózaton
- Az EKG korszerű szolgáltatásai a kormányzati intézmények IT fejlesztéseinek gyorsítására is hatással lesznek
- Biztosított az állampolgárok és vállalkozások számára nyújtott e-ügyintézés infrastrukturája
- A gazdaság élénkítése: az e-ügyintézés és egyéb területekre is serkentőleg hat

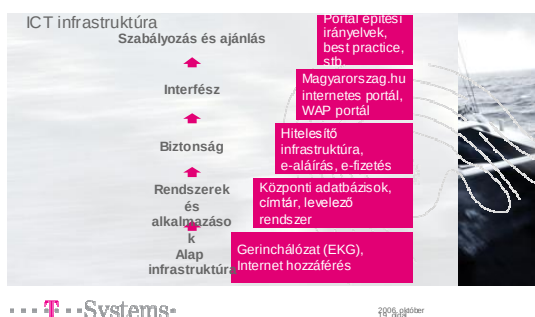
... T Systems

2006. május
17. 08:58

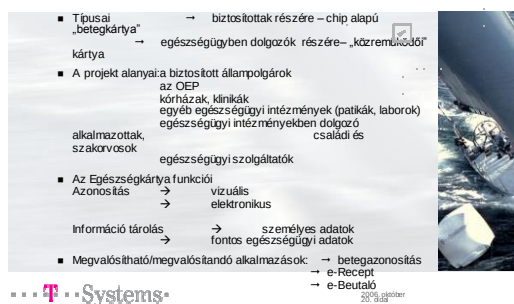
Az elektronikus önkormányzat Stratégiai célok



Az e-önkormányzati infrastruktúra szintjei



Fejlesztési lehetőségek az Egészségügyben Elektronikus egészségügyi kártya



Kommunikáció

A rendszer kiépítéséhez javasolt kommunikációs megoldások

- EKG hálózatra való felcsatlakozás: az OEP, a kórházak és a nagyobb egészségügyi intézmények esetében
- Távmunka jellegű elérés: a kisebb intézmények, szolgáltatók, családi és szakorvosok részére
- Mindkét megoldás előnyei:
 - Telefon és adatforgalmi költségek jelentős csökkentése
 - A forgalmi igények növekedésével a sávszélesség is növelhető
 - Ingyenes Internet-elérés
 - Az EKG hálózaton keresztül más kormányzati intézmények is elérhetők (pl. APEH)



2006. október
21. oldal

... T ... Systems

Köszönöm a figyelmüket !

... T ... Systems

2006. október
22. oldal



Patrice Erulin (Alcatel):
The Network Transformation



Telecom is Embedded in All Future Government Architectures

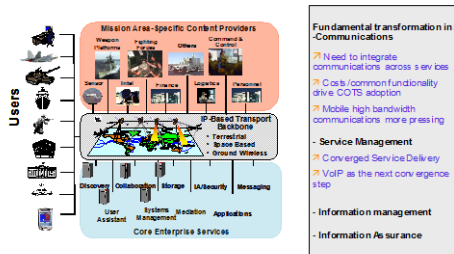
- **Military Transformation**
 - Network-Centric Warfare / Technology as a Force Multiplier
 - Deployed Forces Reachback / Back-Office Collaboration
 - Cross-Agency Information Sharing
 - QoS-centric Networking / Service Based Architectures
 - Outsourced Network Operations
- **Homeland Security**
 - Surveillance and Monitoring / Sensing Networks
 - Cross-Agency Information Sharing
 - Emergency Response Networks
 - Cyber-Security
- **Government Modernization**
 - e-Gov Citizen-to-Government
 - Government Telecommuting
 - Outsourced Network Operations



Alcatel in Defense and Homeland Security - 2 All rights reserved © 2006

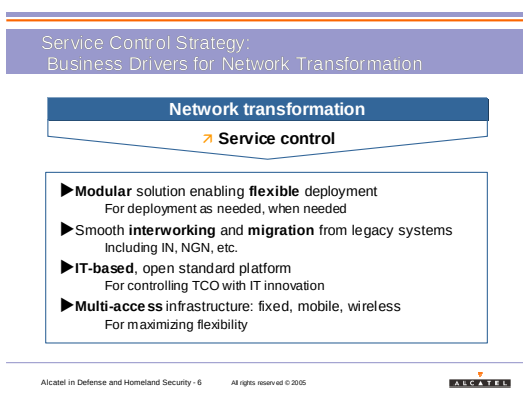
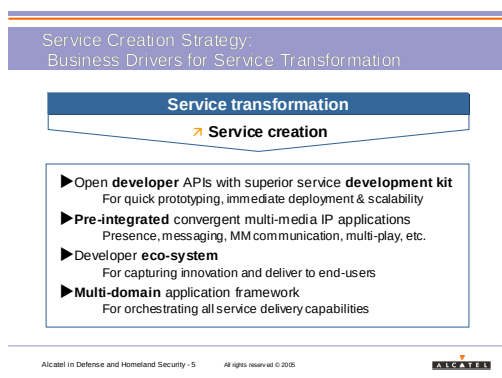
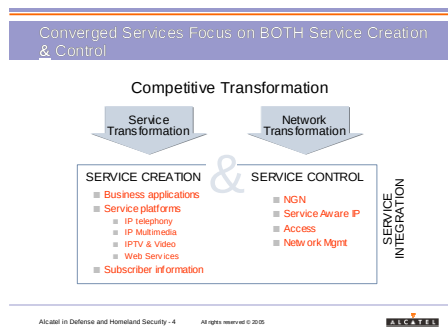


The Network Centric Operations will be ultimately enabled by an IP-Based Transport Backbone and a Converged Services Environment



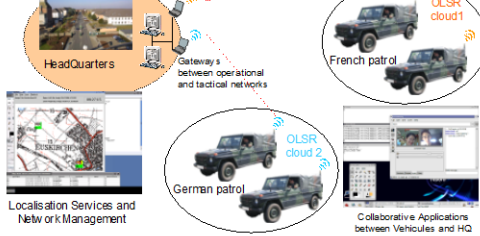
Alcatel in Defense and Homeland Security - 3 All rights reserved © 2006





Example: testing a multi-vendor IPv6/IP mobility solution at CWID 2005 with German armed forces (Euskirchen)

Automatically establishing "self-healing" network, "Moving hot spot",
Ultra-fast deploy



Alcatel In Defense and Homeland Security - 7

All rights reserved © 2005

ALCATEL

Example: Design Study for the Secured Intranet of the French Armed Forces

- Consulting Contract (2ME awarded in December 2005)
- Alcatel, Atos Origin, and Steria in a consortium:
 - Subcontractors: France Telecom, Bertin Technologies, Setec
- Project objective
 - Design the MOD secured intranet
 - Design specifications for phase 1 of the project (16M€ budget) to be purchased at the end of 2006
- Scope of Secured Intranet
 - End-to-end integrated secured communication and information services for 30,000 subscribers covering the full chain of command from government to HQs, and from deployed forces to Command Posts of combat units
- Scope of Consulting study
 - Define architecture & specifications for phase 1
 - Interconnect legacy systems and select the first set of integrated services
 - Define architecture & specifications for phase 2
 - All range of services to be integrated (real time, advanced QoS, SLAs, ...)

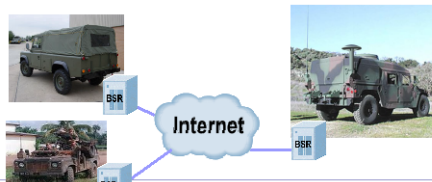
Alcatel In Defense and Homeland Security - 8

All rights reserved © 2005

ALCATEL

Example: The Lucent Technologies portable network solution mounted on land, air or sea-based platforms

- COTS-based Broadband Ad-Hoc Radio Network
 - Based on UMTS/3G and IP Mobility Technologies
 - Autonomous Self-deployment & Self-configuration
 - High bandwidth secure mobile communications
 - High QoS for seamless voice/data/video IP services



Alcatel In Defense and Homeland

All rights reserved © 2005

ALCATEL

Example: the Alcatel WiMAX solution
an IP broadband point to multi-point radio system

➤ Alcatel 9100 – carrier-class performance

- IEEE 802.16-2005 standard (AKA 802.16e)
- Cellular / Nomadic / wDSL modes
- Smart antennas (Adaptive Beam Forming)
- Superior non-line-of-sight capabilities (MIMO)
- Over the air secure encryption (AES/VPN/SSL)

➤ Defense & Security use cases

- Public Safety
- Coast Surveillance
- Critical Infrastructure Protection
- Disaster Recovery
- Deployed army HQs
- Ship to ship, ship to shore

BOARD MEMBER
WIMAX
BTS 30Kg
CPEs

Alcatel in Defense and Homeland Security – 10 All rights reserved © 2005

Example: Operation & Support Services for the Israel Armed Forces

➤ Turnkey **Service Management System** for the Strategic Communications Infrastructure that delivers end to end services over legacy, IP/MPLS, mobile networks

➤ Contract in JV with Ness – 2004/2006

Remote Sites (field, office etc.)

WAN

Core Site/ Data Center

Security Operation Center (SOC)

Network Operation Center (NOC)

Video over IP

IPPBX

IP Phone

Alcatel in Defense and Homeland Security – 11 All rights reserved © 2005

Questions & Discussions

◀ **UNITE YOUR WORLD** ▶ Thank you for your attention

All rights reserved © 2005

Bozsó Zoltán rendőr ezredes:

Rendőri intézkedések rendje a sportlétesítményben és azon kívül

A sportrendezvényeken a rendőrséget (a rendőrt) intézkedési kötelezettség akkor terheli, amikor olyan tény vagy körülményt észlel, illetőleg hoznak tudomására, amely rendőri beavatkozást igényel. **Rendőri beavatkozást igénylő ténynek vagy körülménynek kell tekinteni:**

- a bűncselekményeket,
- a szabálysértéseket,
- felkérésre más személy igazoltatását, ha az igazoltatást kérő valószínűsíti, hogy az igazoltatáshoz jogos érdeke fűződik,
- a közbiztonságra különösen veszélyes anyagok, eszközök lefoglalását, (illetőleg azoknak a rendezvény helyszínére való bevitelének megtiltását, ez a feladat a beléptetést végző személyzet dolga),
- a nyilvános forgalom számára nyitva állóhelyen őrizetlenül hagyott, a közbiztonságra veszélyt jelentő tárgy eltávolítását, megsemmisítését,
- önmagát vagy más veszélyeztető állapotban lévő személy elszállítását, az öngyilkosság lehetőség szerinti megakadályozását, a magatehetetlen, önkívületben lévő személyt lakásra, kijózanító állomásra, egészségügyi intézetbe kísérését, szállíttatását,
- a balesetveszély megelőzése érdekében a közút forgalmának irányítását, korlátozását, illetve szüneteltetését a feltétlenül szükséges mértékben és időtartamra,
- személyeket, illetőleg anyagi javakat közvetlenül fenyegető veszélyhelyzet elhárítását, ennek megszüntetése érdekében terület lezárását, oda a belépés vagy eltávozás megakadályozását, illetve az ott tartózkodók távozásra kötelezését.

A sportlétesítményekben a személyeket és anyagi javakat közvetlenül **fenyegető veszélyhelyzetnek kell tekinteni:**

- a nézőknek az engedélyezett stadionkapacitáson (szektor befogadóképességén) felüli beléptetését, behatolását, összezsúfолódását,
- a szektorokat elválasztók, illetve a játéktérrel a nézőtérrel elválasztó kerítés, a menekülőkapuk mérkőzés alatti bedöntését, átszakítását,
- a feljárók, lépcsők eltorlaszolását, lelátók, korlátok, támfalak, kerítések, állványzatok, oszlopok túlterhelését, megrokkadását, a lezuhanás, omlás vagy leszakadás közvetlen veszélyét,
- az építmények, berendezési tárgyak tömeges méretű, felfegyverkezésre irányuló megbontását, megrongálását,
- a szurkoló táborok között vagy azokon belül kialakuló tömegverekedéseket,
- a csapatok, játékevezetők illetve más közreműködők elleni közvetlen támadást,
- a keletkezett tüzek terjedését.

A biztosítás parancsnoka

- köteles a rendezvényen jelen lenni, figyelemmel kísérni a közönség magatartását,
- a létesítmény belső rendjét sértő cselekmények esetén hívja fel a szervező figyelmét a rend helyreállítására,
- intézkedjenek a rendőri beavatkozást igénylő körülmények esetén a szükséges erők átcsoportosítására, helyszínre irányítására, a szükséges intézkedések megtételére,
- soron kívül tegyen jelentést a rendőri szerv vezetőjének és az ügyeleti szolgálatnak minden olyan eseményről, amely tömeges rendbontást vagy jogsértést valósít meg, amely a létesítmény egy részének vagy egészének kiürítését, a rendezvény megszakítását, a rend fenntartásához vagy a közlekedés rendjének biztosításához további rendőri erők vagy társ szervek helyszínre irányítását teszi szükségessé.

A közbiztonságra leginkább veszélyes szurkolói csoportok elhelyezésére szolgáló, külön kijelölt szektor a szomszédos szektoroktól elválasztó kerítés mentén belülről sorfalszolgálattal is biztosítható. A jogsértő cselekmények és a jogsértő személyek felderítése, azonosítása, a nyílt rendőri erők helyszínre irányításának segítése érdekében a szektorokban polgári ruhás rendőrök helyezhetők el. Megfelelő fedésükről, védelmükről, a rejtett összeköttetés biztosításáról, felismerési jelekről, nagyobb erejű beavatkozás esetén előzetes kívánásukról gondoskodni kell. A létesítményen belül és kívül széleskörűen kell alkalmazni a rendelkezésre álló képrögzítő dokumentációs eszközöket. Ezek kezelői önállóan vagy a biztosításparancsnok (kijelölt szolgálati csoport parancsnoka) utasítására a személyazonosítást később is lehetővé tévő módon rögzítsék a jogsértő személyt és az általa elkövetett jogsértést, ennek megtörténtét jelentsék (jelezzék). Vegyék fel a rendőri beavatkozást, valamint - *az összehasonlítás érdekében* - készítsenek felvételt az elfogott (előállított) személyről is. A fenti feladatokat több dokumentációs csoport is végezheti. A képi anyagok összerendezését, az eljárás alapjául szolgáló iratokhoz csatolását az elszámloltató csoport végezze. Azokban az esetekben, amikor a jogsértő személy kiemelése nem lehetséges, és a helyszínen videó printer vagy más képmásoló berendezés áll rendelkezésre, a jogsértő fényképét a szükséges példányszámban el kell készíteni, a szolgálati csoportoknak ki kell adni, majd a rendezvény befejezése után, a közönség eltávozásának időszakában kell végrehajtani az elfogást. A szektorokból, csoportosulásokból a jogsértő személyek kiemelésére kiemelő csoportot kell alkalmazni. A kiemelő csoport állománya a beavatkozáshoz alkalmas ruházatot és egyéni védőeszközöket viseljen, ereje egy rajtói (6 fő) egy szakaszig terjedhet. Indokolt esetben, több célszemély egyidejű kiemelésére több kiemelő csoport összevontan is alkalmazható. A

kiemelést a biztosítás parancsnoka vagy külön felhatalmazás alapján a kijelölt biztosító csoport (szektor) parancsnoka rendelheti el. A kiemelő csoport részére pontosan meg kell határozni a jogsértést elkövető személy tartózkodási helyét, eltávozásának irányát, személyleírását, a jogsértő cselekményt, a környezetében tartózkodók hangulatát, magatartását, viszonyát a jogsértő személyhez. Amennyiben lehetséges, a kiemelő csoport parancsnoka részére gyorsfényképet is biztosítani kell. A tájékozódás elősegítése érdekében a tömeg körül jól látható tereptárgyak segítségével tájékozódási pontok is kijelölhetők. Csoportos előállításához a szükséges szállítóeszközöket és arra alkalmas helyiségeket előzetesen ki kell jelölni és erre a célra alkalmassá kell tenni.

A nagyobb erejű tartalékokat, beavatkozásra kijelölt szolgálati csoportokat, technikai eszközöket a tömeg által nem látható helyen, rejtve, de a gyors beavatkozásra alkalmas módon, felszerelve kell elhelyezni. A sportrendezvény alatt, azt megelőzően vagy azt követően egy meghatározott területrészen vagy egészében történő kiürítésének, csoportosulás feloszlatásának elrendelésére a biztosítás parancsnoka jogosult

- a személyeket vagy anyagi javakat közvetlenül fenyegető veszélyhelyzet megszüntetésére,
- tömegesen tanúsított jogellenes magatartás esetén, amennyiben a tömeg a jogellenes tevékenység befejezésére, jogkövető magatartásra vagy a szétoszlásra irányuló rendőri felszólításnak nem tesz eleget.

A **sportrendezvény befejezését követően** a szurkolótáborok elválasztása és az erőszakos cselekmények megelőzése érdekében a közönség egy része meghatározott ideig a létesítményben visszatartható. A visszatartás nem hiúsíthatja meg a menetrendszerű tömegközlekedési eszközök elérését, a szurkolók akadálytalan elutazását. A visszatartás okáról, várható időtartamáról a közönséget tájékoztatni kell. Az előállított és őrizetbe vételre nem kerülő személyekkel szemben a szükséges eljárásokat lehetőleg úgy kell lefolytatni, hogy elbocsátásukat követően a mérkőzés után induló menetrendszerű tömegközlekedési járműveket elérhessék.

Megyeri Sándor (VT-Rendszertechnika Kft.)

A Magyar Honvédség követelményei alapján kifejlesztett
20'-as zárt felépítmény család

VT-Rendszertechnika Kft.

**A MAGYAR HONVÉDSÉG követelményei alapján
kifejlesztett**

20'-as zárt felépítmény család többcélú felhasználásra

Előadó: Megyeri Sándor

Ügyvezető igazgató

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM

Kommunikáció 2006

Nemzetközi szakmai tudományos konferencia

2006.okt.25.

VT – RENDSZERTECHNIKA Kft. Székesfehérvár

INTEGRÁLT TERMÉKEK és GYÁRTÁSI SZOLGÁLTATÁSOK



Honlap : www.vtsys.videoton.hu

VT-Rendszertechnika Kft.

TÖBB ÉVES TAPASZTALATTAL RENDELKEZÜNK AZ ALÁBBI TERÜLETEKEN

-Konténer gyártás

-Telekommunikáció

-Védelmi elektronika

-Mechanikus és elektromos műszerek kalibrálása



VT-Rendszertechnika Kft.

Konténer gyártás

A VT-Rendszertechnika 1995 óta fejleszt és gyárt tűzihorganyzott konténereket különböző vásárlói igényeket, kéréseket figyelembe véve. A berendezések a megrendelő által meghatározott szempontok figyelembevételével és betartásával kerülnek kiválasztásra. Ezek a konténerek teljes biztonságot nyújtanak a rossz időjárási viszonyok és az erős szél behatolók ellen. Az energia ellátás történhet hálózatról vagy aggregátorról. A VT-Rendszertechnika Kft. kifejlesztett egy NATO kompatibilis konténer családot is. Ennek szerkezete lehet tűzihorganyzott acél vagy hegesztett alumínium.

Általános tulajdonságok:

- Víz bázisú környezetbarát festés
- Hőszigetelt és légkondicionált belső tér
- Speciális riasztó rendszer
- Speciális beépített rendszer és zár
- EMC/EMP védelem (TEMPEST)

Tűzihorganyzott acél konténer

Mobil telekommunikációhoz: - Vodafone típusú
- T-Mobile típusú

Katonai felhasználásra: - Hegesztett alumínium konténer

- KS-20

- KT-20

- KC-20

- MLK-Mobil Biológiai Labor Rendszer

VT-Rendszertechnika Kft.

Hegesztett alumínium konténer



VT-Rendszertechnika Kft.

Hegesztett alumínium konténer



VT-Rendszertechnika Kft.

KS20 tűzihorganyzott acél konténer



VT-Rendszertechnika Kft.

KS20 tüzhorganyzott acél konténer



VT-Rendszertechnika Kft.

KS20 tüzhorganyzott acél konténer



VT-Rendszertechnika Kft.

KT20 tűzihorganyzott acél konténer

EMC/EMP védett



VT-Rendszertechnika Kft.

KT20 tűzihorganyzott acél konténer

EMC/EMP védett



VT-Rendszertechnika Kft.

KT20 tüzhorganyzott acél konténer

EMC/EMP védett



VT-Rendszertechnika Kft.

KC20 tüzhorganyzott acél konténer



Dr. Medveczki Zoltán orvos őrnagy

Életmentő beavatkozások fül- orr- gége sérülések esetén

A fej- nyak, ezen belül a fül- orr- gége régió sérülései a sérülések 15-30 százalékában fordulnak elő, esetükben gyakran számolni kell az egyidejű polytraumatizációval (3). Ellátásuk speciális felkészültséget igényel, több társszakma együttműködését igényli (4). A túlélés szempontjából kritikus jelentőségű a légzési elégtelenség azonnali felismerése, majd e régióban fellépő vérzés csillapítása. A „damage controll surgery” (DCS) elveinek figyelembe vételével életmentő beavatkozásnak számít a sérülés következtében fellépő szövődmények megelőzése, a maradandó károsodások elhárítása.

A sérültet ellátó orvosnak hármas feladata van :

1. a sürgősségi diagnózis felállítása,
2. a vitális funkciók megtartása,
3. döntenie kell az ellátás sorrendjéről.(1)

A diagnózis felállításához elengedhetetlen a fül-orr-gégészeti szakmai irányelvek és algoritmusok maradéktalan ismerete, biztosítani kell a kor színvonalának megfelelő kiegészítő vizsgálatok elérhetőségét.(2)

Fej- nyaki sérülteknél életmentő beavatkozást ABC (NATO terminológia) szerint végzünk (7):

A (airway): szabad légút biztosítása

B (bleeding): vérzés csillapítás

C (complete assesment): a sérült további teljeskörű vizsgálata és ellátása a DCS (damage control surgery) elveit alkalmazva

A fej- nyak sérüléseket három csoportra osztjuk fel:

- I. Az arckoponya sérülései
- II. Nyaki sérülések
- III. A koponya alap, os temporale, fülészeti régió sérülései (8)

I. Az arckoponya sérülésein az arcközép, állcsont, orrcsont, naso-orbito-ethmoid régió, fronto-basis töréseit, a szájüreg, a garat, az orrmelléküregek sérüléseit, lágyrész sérüléseket, ezen belül az arcideg és a ductus parotídeus folytonosságának megszakadását értjük.

Azonnali teendők az arckoponya sérülteknél ABC szerint:

A (airway): a szabad légút biztosítása

A bifurcatio trachea feletti légúti elzáródás stridoros légzéssel jár. Arckoponya sérülése esetén a fellépő stridor okai a következők lehetnek:

- a sérülés következményeként fellépő ödéma vagy bevérzés,

- állcsont törés esetén a nyelv tamponálhatja a hypopharynxot,
- a tört, szabadon flotáló maxilla hátra eshet,
- kitört fog és egyéb idegentest jelenthet légúti akadályt.

A légúti elzáródás megszüntetésére a következő lépéseket tegyük (5):

- idegentest eltávolítása a szájüregből, garatból,
- az állcsont, a nyelv előrehúzósa,
- az arcközép csont kiemelése,
- nasopharyngeális vagy oropharyngeális tubus behelyezése,
- endotracheális intubáció lélegeztetéssel,
- conicotomia vagy sürgős tracheotomia.

A szájüreg áttekintése során a látható idegentesteket kézzel eltávolítjuk. Ügyelni kell arra, hogy ujjunkat szorosan a szájüreg oldalsó fala mentén vezessük be, és a középvonalban húzzuk ki, így kerülve a légúti akadály mélyebbre jutását. A fulladást okozó hátra-lefelé diszlokált arcközép előemelése a felső fogak megragadásával, vagy szájon keresztül a keményszájpad mögé nyúlva végezhető el. A hátraesett állkapocs kiemelése két kézzel az állkapocs szögleteknél fogva történik. Fulladást okozhat a hátraesett nyelv is, melynek előemeléséről legegyszerűbben a nyelv hátba öltött vastag fonállal gondoskodhatunk. A fonalat az alsó frontfogakhoz rögzítjük. A garatba ékelődött idegentestet eltávolítjuk. Az orrgaratba idegentest csak ritkán kerül, azonban eszméletlen sérültnél hányás kapcsán a nyelöcsőben, illetve a gyomorban lévő idegentest az orrgaratban megakadhat. Kimutatása, eltávolítása sokszor nagy gondot okoz. Amennyiben az idegen testet eltávolítani nem tudjuk és a sérült légzése gátolt, conicotomiát végzünk.

Conicotomia

Hirtelen fellépő fulladás esetén nincs módunk és időnk tracheotomiát végezni. Ilyenkor conicotomiát alkalmazunk. A nyak közepén kitapintjuk a gyűrűporc és a pajzsporc között a ligamentum conicumot, felette a bőrt hosszanti metszéssel átvágjuk, és a kéznél levő eszközzel beszűrünk a ligamentum conicumba. A conicotomiás nyílásba helyezett kanül 2-3 napnál tovább nem tartható fenn, ezért, ha a fulladás oka nem szűnt meg, tracheotomiát alkalmazunk (4).

Tracheotomia

A sürgős műtétet infiltrációs érzéstelenítésben végezzük. A sérültet hanyattfekvő helyzetbe helyezzük. A bőrmetszést a középvonalban ejtjük a pajzsporc alsó szélétől lefelé 3-5 cm-re. A subcutis és a platysma átvágása után megkeressük a linea albát. Itt a fasciákat és izmokat a középvonalban szétválasztva elkampózzuk. Felül a pajzsmirigy isthmusa szalagosan tapad a pajzs-

porcon és fedi a trachea felső részét. Ezt a szalagot át kell vágni. A pajzsmirigy isthmusát két lefogás között átvágjuk, azokat elvarrjuk. A II. trachea porcánál bemetszve 7-8 mm-es hosszanti babérlevél alakú darabot kimetszünk a tracheából és az így képzett stomába helyezzük be a kanült. A kanült gézzel vesszük körül a subcutan emphysema megakadályozására, a bőrsébet 1-2 varrattal szűkítjük. A kanült és a sebre helyezett bevágott gézt kötéssel rögzítjük (4). A szabad légút biztosítás során különös figyelmet kell fordítani a nyaki gerinc állapotának felmérésére. Az arckoponya tompa sérüléseinek tíz százalékában számíthatunk a nyaki gerinc sérülésére is, ezért eszméletlen betegnél annak immobilizációja szükséges. Eszméleténél lévő betegnél kötelező elvégezni a nyaki gerinc vizsgálatát (7).

B (bleeding): ér sérülések ellátása, vérzéscsillapítás

Az arc sérülései jelentős vérzéssel járhatnak. Elvérzéssel fenyegető súlyos vérzés leggyakrabban az a. carotis communisból és a v. jugularis internából észlelhető. A vérzés csillapítás progresszív módon történik a sebre gyakorolt nyomástól a vérző ér lekötéséig. Amennyiben a vérzéshez nem férünk hozzá, a régiót ellátó főütőeret, az a. carotis externát kell leszorítani. Az értörzset a pajzsporc felett, a m. sternocleidomastoideus elülső szélé mentén a nyakcsigolyához nyomjuk. Az a. carotis externa megfelelő ágainak (a. temporalis superficialis, a. facialis, a. lingualis, a. labii), de szükség esetén magának az a. carotis externának a trigonum caroticum területén való lekötése is elkerülhetlenné válik(3). Preparáláskor az a. carotis externa és interna elkülönítésére egyetlen biztos támpont, hogy a a. carotis externa oldalágakat ad, míg az a. carotis internának extracraniálisan nincs oldalága. Az a. carotis externa lekötése vérellátási zavart nem okoz, mert a régióknak kiváló kollaterális hálózata van. A nyelv erős vérzése esetén a nyelvgyök leszorítása, illetve az a. carotis externa leszorítása, lekötése válik szükségessé. Orrvérzés esetén elülső vagy hátsó tamponádót (réteges, illetve Belloque tampon) kell alkalmazni. Nasalis liquorrhoea esetén nem szabad az orrot tamponálni meningitis veszélye miatt. Az oropharynx és pharynx kitamponálását csak intubált sérültnél végezhetjük el. Érleszorítót vakon ne használjunk, mivel így könnyen okozhatjuk az arcideg és a parotis ductusának sérülését.

C (complete assesment): további sérülések felmérése, szövődmények megelőzése

A sérült állapotának stabilizálása után a sérülés kiterjedésének, mélységének felmérésekor megteesszük a szükséges lépéseket a szövődmények kizárása céljából a CDS elveit szem előtt tartva. A sürgősségi diagnózis felállításához szükség van a koponya röntgen és CT vizsgálatára.

Az orbitakeret, arccsont, orrcsont, állkapocs és homlok vizsgálata során - a kóros mozgathatóság, elmozdulás, lépcsőképződés, paresztésia, diplopia, szemhéjak duzzanata, exophthalmus, haematoma, emphysema, retropharyngealis haematoma, vérzés (a. maxillaris, a. ethmoidalis), anosmia, nasalis iquorrhoea - azok törésére, az orrmelléküregek (sinus frontalis, sinus maxillaris) és a frontobasis sérülésére utal. Az orrcsonttörés mellett az orrsővény traumás elferdülése is előfordul, mely megfelelő ellátás nélkül elfertőződhet (abscessus septi nasi). Nasalis liquorrhoea jön létre, ha az orrüreg és a subarachnoidalis tér között összeköttetés alakul ki a lamina cribrosa törése folytán (4). Amennyiben az orrgyök ellaposodott és a mediális szemzugok közötti távolság több mint 40 mm a naso-orbito-ethmoid régió (NOE) törése állhat fent. NOE, illetve nasalis liquorrhoea esetén az orrban történő manipuláció (orr tamponálása) tilos, mivel a lamina cribrosa sérülése miatt nagy az agyi contaminatio veszélye. Az arckoponya sérülései vagy az orrmelléküregek, vagy a szájüreg, vagy a külvilág felé nyitottak, ezért a gram-pozitív törzseket lefedő antibiotikum és tetanus elleni prophylaxis szükséges(3). Ugyancsak antibiotikum kezelés szükséges nasalis liquorrhoea esetén. Az agyidegek vizsgálatakor ellenőrizzük a látás, a hallás, az arcizmok működését, a szemek és a nyelv mozgását. Az arckoponya területén lévő kisebb lágyrész sérüléseket azonnal ellátjuk. A csontsérülések és a velük járó súlyos lágyrész sérülések ellátása 24 órán belül halasztható. A sebből kiálló idegentest eltávolítása a sérülés helyszínén csak akkor megengedett, ha az okozza a fulladást, vagy a vérzéscsillapítást akadályozza. A szájüreg és a garat áthatoló sérüléseit többrétegű varrattal zárjuk. Nyálkahártya sérülés suturát nem igényel. A nyelv harapásos sérülései általában felszínesek és spontán gyógyulnak. Mélybe terjedő harapott sebek esetén többrétegű varrat, kisebb nyelvdarabok teljes leszakadásakor reimplantáció szükséges. A légút biztosítás, vérzéscsillapítás mellett gondoskodnunk kell a fájdalomcsillapításról és a zavartalan folyadékptólásról. Szükség lehet a labilis helyzetben lévő tört arccsontok ideiglenes rögzítésére. Sebkötőzésre az általános elvek az irányadóak.

II. Nyaki sérülések

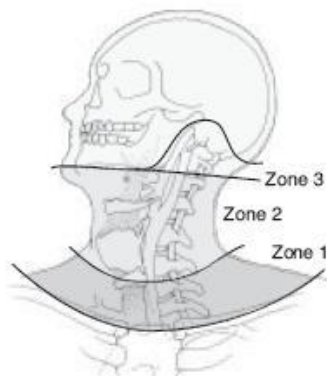
A nyaki sérülések lehetnek tompák és áthatolóak. Az áthatoló nyaki sérülések a gége, a nyelőcső, a légcső, az a. vertebralis, az a. carotis ext., int. és a v. jugularis int. sérülésével járhatnak együtt. Nagyér sérülés az esetek 20 százalékában, a légút és a tápcsatorna nyaki szakaszának sérülése az esetek 10 százalékában fordul elő. A sérülés következményeként beálló halál oka elsősorban az elvérzés. Fulladással veszélyeztet a gége és a légcső sérülése. Halálos kimenetelű lehet a nyelőcsősérülés következtében fellépő mediastinitis, sepsis.(7) Nyaki sérülések esetén életmentő beavatkozásnak minősül a szabad légút biztosítása, a vérzéscsillapítás, valamint a szövödmények, a maradandó

károsodások elkerülése miatt végzett sebellátás a DCS elvei szerint. A legfontosabb klinikai jelek, amelyek áthatoló nyaki sérülésre utalnak:

- jelenleg is fennálló, ill. az anamnézisben jelentős vérzés
- növekvő haematoma
- hypotensio, cyanosis
- hiányzó vagy csökkenő pulzus a nyakon, karokon
- helyi neurológiai deficit, a pszichés állapot megváltozása
- haemotorax vagy a mediastinum kiszélesedésének radiológiai jelei
- crepitatio vagy subcutan emphysema
- levegő buborékok, étel és nyál a sebben
- nehézlégzés vagy stridor
- érzékenységi, fájdalom a trachea felett, fájdalmas nyelés
- rekedt, abnormális hang, vérhányás, vérköpés
- nyaki és brachialis plexus lesio, Horner syndroma, nyelv deviatio, n. laryngealis és recurrens sérülések, n. facialis paresis, rekeszizom paralízis

A diagnózis felállításához segítséget ad a nyak natív röntgen felvétele, amely kimutatja a szervek és a légoszlop elmozdulását. A mellkas röntgen felvétel kiszélesedett mediastinumot, dissekaló emphysemát, pneumothoraxot, haemothoraxot, gerinctörést jelezhet. Arteriographia, kontrasztanyagvizsgálatok és endoscopia végzendő minden esetben, ahol gerinc, vaszkuláris, légúti, pharyngo-oesophagialis sérülésre van gyanú (4).

A nyakat diagnosztikai és az ellátás szempontjából három zónára osztjuk fel:



1. zóna: a claviculától a membrana cricoideáig terjed, tartalmazza az arteria és vena subclaviát, az arteria carotis communist, a plexus brachialist, a tüdő felső lebenyét

2. zóna: a membrana cricoideától a mandibula angulusáig, amelyben megtalálható az arteria carotis communis, a vena jugularis interna, az oesophagus és a trachea

3. zóna: a mandibula angulusától a koponya alapig húzódik, itt az arteria carotis interna fut

Műtégi stratégia:

Sértetlen platysma esetén műteti beavatkozás nem szükséges.

A nyak 2. zónájának sérülése esetén a musculus sternocleidomastoideus el-
ülső felszíne mentén történő metszésből a nagy ereket, tracheát, oesophagust lehet feltárni.

Az 1. és 3. zóna sérüléseit a klinikai és radiológiai vizsgálatok alapján látjuk el. Műteti feltárást az ér sérülésnek megfelelően végzünk.

A gége sérülésének azonnali ellátása:

A gége sérülhet izoláltan, vagy nyaki sérülések részeként. Néha csak a rekedt hang jelzi a gége sérülését. Súlyosabb esetekben asphyxia léphet fel a légutak elzáródásától. Ez történhet a gége elmozdulással járó sérülései, leszakadt darabok, idegentestek a gége ürterébe ékelődése, vérzés, véralvadék és a fellépő ödéma miatt. Az állapot azonnali intubációt, conicotomiát vagy tracheotomiát követel meg a légúti idegentestek eltávolítása után. Az intubáció a sérült gége beszűkülése miatt nehézséget okozhat. A gégeből, hypopharynxból eredő vérzést a garat gézcsíkkal történő tamponálásával csillapítjuk. Conicotomiát, tracheotomiát eszméleténél lévő sérültnél helyi infiltrációs érzéstelenítésben végzünk. A fenyegető gégeoedéma kivédésére szisztémás szteroid adása ajánlott.

Azonnali teendők trachea sérülés esetén:

A nyak 2. zónájának sérülése esetén sérül leggyakrabban a trachea. A fenyegető asphyxia miatt a tracheostomiás tubust a tracheafal sérülésén keresztül vezethetjük be. A tracheát 5 cm hosszan lehet resecálni. End to end anastomosissal egyesíthetjük a mobilizált trachea végeket lehetőleg megkímélve a laterális fal vérellátását(10).

A vérzések ellátása áthatoló nyaki sérülés esetén(9):

1. Szájüregi vérzések ellátása:

A fossa tonsillaristól laterálisan áthatoló sérülés gyakran okozhatja az arteria carotis externa, annak ágai és a carotis interna rejtett sérülését. Angiographia, CT vizsgálat elvégzése szükséges. Az arteria carotis externa ágai szabadon leköthetők, végső esetben az interna lekötése is szükségessé válhat.

2. Az artéria vertebralis sérülésének ellátása:

Ha az arteria carotis communisra gyakorolt nyomás ellenére sem csillapodik a nyak posterolateralis sérüléséből eredő vérzés, az arteria vertebralis sérülésére kell gondolnunk. Preoperatív angiographia tisztázhatja a sérülés helyét és a contralateralis artéria épségét (aplasia a baloldalon gyakori). Amennyiben a contralateralis artéria sértetlen, úgy a sérült ág proximalis vagy distalis leköttése szükséges. A vérzéscsillapítás történhet csontviasszal vagy Foley katéterrel.

3. Az arteria carotis interna sérülésének ellátása

A vérzést a hemiplegia és mély coma kialakulásáig kell ellátni. Az artéria carotis interna végső esetben leköthető. Carotis shunt használata 24-48 óráig ajánlott. Kisméretű perforációt 6,0 polypropylénnel varrjunk össze. Nagyobb kiterjedésű ér sérülés esetén end-to-end anastomosis, vena graft interpositio, arteria. carotis externa interpositio végezhető.

4. A vena jugularis interna sérülésének ellátása:

A laterális varratot részesítsük előnyben. Ha a contralateralis vena ép, úgy a sérült ág leköthető.

Az oesophagus sérülésének ellátása (6):

Az oesophagus sérülésének megállapítása nehéz, az esetek 25 százalékában aszimptomatikus lehet. A nem diagnosztizált nyelőcsősérülés halálhoz vezethet. Debridement után a sebzárást egysoros felszívódó varrattal végezzük. Izomlebennyel való zárás védelmet biztosít a sipoly kialakulásával szemben. A drenázst szívó drainnel biztosítjuk. Mesterséges táplálás, antibiotikum adása szükséges.

III. Koponya alap, os temporale, fülészeti régió sérülései

1. Külsőfül sérülése
2. Középfül sérülése
3. Belsőfül sérülése

A fül sérülései gyakoriak, de általában a külsőfül szakított, zúzott, tépett sérüléseire korlátozódnak. A középfül és belsőfül légnyomás által okozott sérülései gyakran későn kerülnek felismerésre. A halántékcsont és a sziklacsont törései különböző mértékű közép- és belsőfül sérülést okozhatnak. A belsőfület károsító akusztikus trauma hirtelen hallásvesztéssel, heves vegetatív tünetekkel jár. ABC terminológia szerint életmentésről a fülészeti régió sérüléseinek nem beszélhetünk, de ha a C pont (complett assesment), vagyis a teljességre törő diagnosztizálás, a DCS elvei szerinti ellátás, szövődmények megelőzése

se, maradandó károsodás elhárítása nem valósul meg, úgy ezek a sérülések elhúzódó betegséghez, maradandó károsodáshoz vezethetnek.

Külsőfül sérülései

A legfontosabb sérülések a contusio, le- és elszakadás, valamint az égés és fagyás.

Szövődmények:

A porc és porchártya között kialakult haematoma elfertőződhet, elgennyedhet, perichondritis, porcnekrosis alakulhat ki. A hallójáratí sérülések később stenosis, atresia okozhatnak.

Ellátás: Szabályos sebtoalett után vérző seb esetén nyomó-, egyébként fedőkötéssel látjuk el a sérült fület. Vérző hallójárat esetén a hallójáratot tilos tamponálni, mert a vérzés a középfülből is származhat. Ilyenkor vattával ellátott fedőkötetést alkalmazunk. A leszakadt kagylódarabokat jégbe hűtjük. A fülkagylón kialakult othaematomát megpungáljuk, leszívjuk, majd a sérülés helyére nyomókötést helyezünk (4).

Középfül sérülései

A legfontosabb sérülések lehetnek: dobhártya perforatio, os temporale törése, os pyramidale törése, n. facialis sérülése. A diagnosztizáláshoz kétirányú koponya, Schüller, Stenvers röntgen felvételekre, audiológiai (vizsgálatra, CT felvétel készítésére van szükség.

A dobhártya traumás perforálódása vezetékes típusú halláscsökkenéssel, fájdalommal, fülzúgással, esetleg vérzéssel jár.

Az os temporale törései változó mérvű középfül sérülést okozhatnak.

Sziklacsont törések járhatnak dobhártya perforációval, vagy anélkül. Amennyiben perforáció történt a hallójáratban vérzés, liquorcsorgás látható, ha nincs perforáció a dobhártya kékes fekete színű a dobüregben felgyülemelő vértől (haemotympanon). Amennyiben a belsőfül is sérül a halláscsökkenés kevert típusú.

Az arcideg sérülhet a canalis facialisban, vagy a belső hallójáratban. Eszméleténél lévő sérültnél fel kell mérni és dokumentálni az arcideg minden ágának működését. Az arcideg bénulás kialakulásának kezdete (akut, ill. késői) fontos a kezelés és a sérülés kimenetele szempontjából. Akut kezdet az arcideg szakadását jelzi. Amennyiben az arcideg bénulás a sérülés gyógyulása után is fennáll, a bénulás magasságát kell meghatározni. A canalis facialisba duzzadt ideg decompressio útján szabadítható fel (7).

Ellátás: Hallójáratí vérzés, liquorcsorgás esetén a hallójáratí tamponálás tilos. Antibiotikum, Tetanus AT adása szükséges. A sérült további intézeti ellátásra szorul. Az arcideg bénulás kialakulásának kezdete (akut, ill. késői) fontos a kezelés és a sérülés kimenetele szempontjából. Akut kezdet az arcideg szaka-

dását jelenti. Amennyiben az arcideg bénulás a sérülés gyógyulása után is fennáll, a bénulás magasságát kell meghatározni. A canalis facialisba duzzadt ideg decompressio útján szabadítható fel.

A belsőfül sérülései

Leggyakoribb formái a labyrinth commotio, akusztikus trauma, kinetózis, a sziklacsont haránttörése

Labyrinth commotio: fejsérülések során indirekt erőművű behatásra mindkét oldali belsőfül károsodhat. A hallószervet érő sérülés idegi eredetű halláscsökkenést, az egyensúlyozó szervet érő sérülés egyensúlyzavart, pozicionális nystagmust okoz.

Akusztikus trauma: a fület ért egyszeri, igen heves, rövid impulzusszerű zajbehatás olyan heves peri- és endolympha mozgást válthat ki, hogy a Corti szervnek kisebb, nagyobb szakasza sérülhet. Halláscsökkenéssel, heves fülzúgással jár.

Kinetózis: a belsőfül vestibularis részének élettani ingerekkel történő, de szokatlan erősségű és huzamos ingerlése, mely vestibularis izgalmi tüneteket vált ki. A tünetek között a vegetatív jelek dominálnak (hányás, hányinger, szédülés, verejtékezés, sápadtság, gyengeség érzés, bradycardia, hypotonia, collapsus hajlam).

A sziklacsont haránttörése esetén a labyrinthuson és a belső hallójáraton megy át a törésvonal. A halláscsökkenés idegi eredetű, kifejezett szédüléssel és nystagmussal.

Ellátás: A sérült fektetést igényel. Hányáscsillapító, keringésvajító infúziós kezelésre szorul.

Irodalom:

1. Dr Bencze B.- Dr Göbl G. : Oxiológia Budapest, Medicina, 1997.
2. Fül-orr- gégészeti szakmai irányelvek és algoritmusok Budapest, Fül-, orr-, gégégyógyászat 48, 1. Suppl. , 2002.
3. Dr Gyenes V. : Maxillofacialis sérülések ellátása ROLE 1 és ROLE 2 szinten, Honvédorvos 2001. 3-4. szám
4. Dr Heid L. , Dr Kollár D. : Fül-orr-gégészeti ellátás ROLE 1 és ROLE 2-ben, Honvédorvos 2001. 3-4. szám
5. Dr Medveczki Z. , Dr Horváth E.: Fül-orr-gégészeti ellátás sürgősségi osztályon, Honvédorvos 2005.
6. Dr Medveczki Z. , Dr Horváth E. : Fej-nyak sebészeti ellátás minősített helyzetben, Honvédorvos 2006.
7. NATO Handbook of Emergency War Surgery, 2005.
8. Orgován Gy. , Dr Farkas J. : Katona- és katasztrófaorvostan alapjai



Small Dimetra IP Compact system
Do you speak digital?



Szvéték Ferenc (FERCOM): Small Dimetra IP Compact system

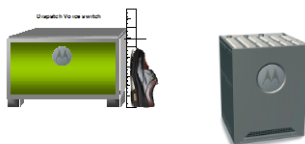


Small Dimetra IP Compact system
Do you speak digital?

Fercom

Small Dimetra IP Compact system
Do you speak digital?

Kicsi de hatékony infrastruktúra



RF Sites Using Dimetra IP Base Stations

Optionális tulajdonságok

- Redundáns vezérlő
- Adatszolgáltatások
- Telefonia
- Biztonság



- MTS-4**
- 4 vivő (8-ra bővíthető)
 - Hatékony és megbízható
 - Teljes redundancia
 - Csúcs teljesítmény

- MTS-2**
- 2 vivő (4-re bővíthető)
 - Kompakt és könnyű
 - Könnyen bővíthető
 - Teljes körű funkcionális

Tulajdonságok és kapacitás

- Teljes DIMETRA A IP tulajdonságok
- 1-12 cella, 8000 kbps
- Short & packet data
- 12 kbps (12 kbps)
- 1-2 kbps (12 kbps)
- Security: End to End Encryption and Air Interface Encryption
- Minden frekvencia sávban
- Egyszerű telepítés és karbantartás



Egyszerű karbantartás, versenyképes szolgáltatások

- Előre konfigurálható
- Felhasználó igényeihez igazított
- Könnyű telepítés

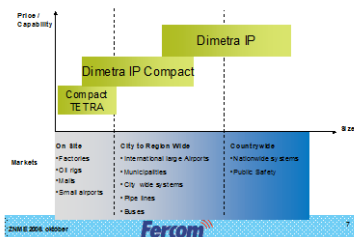


Versenyképes szolgáltatások



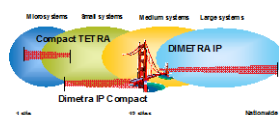
A siker kulcsai:
műszaki tulajdonságok
és lehetőségek
szüksége

Motorola TETRA Portfólió



Összegzés

- 1-12 cella
- Könnyű átjárhatóság a nagy DIMETRA rendszerek felé
- Újra felhasználható eszközök
- Dimetra IP Compact azoknak a felhasználóknak a legjobban megfelel, akik több lépésben (költséghatékonyan) akarják megvalósítani rendszerüket





Köszönjük a figyelmet!



Szvéték Ferenc

szvetek.ferenc@mail.fercom.hu

www.fercom.hu

TETRA

- Integrált Motorola TETRA Modem
- SOS és Multi-Slot PowerID-azs
- 1W adó teljesítmény

WiFi

- Opcionális 802.11g vezeték nélküli modem
- Helyi csatlakoztatás, készülék szinkronizáció
céljából vagy más hálózattal

Bluetooth & IrDA

- Bluetooth és infravörös csatlakozási lehetőség
- Kiegészítő és egyéb eszközök
csatlakoztatási lehetősége



- 1 GB RAM with 40 GB Hard Drive
- Windows XP operációs rendszer
- USB 2.0, serial, digital video I/O
- Nagyméretű 12.1" érintőképernyő

- Integrált ujjlenyomat olvasó
- MIL-STD-810F szabványnak megfelelő
magnézium ház



2009. 06. 01. szerda



22

2009. 06. 01. szerda



23



Jean-Louis DEBEURET (THALES):
Tactical Internet et Postes de Commandement

Mesdames et messieurs,

C'est un grand honneur et un privilège pour la société Thales de pouvoir s'adresser à vous dans le cadre de cette conférence annuelle sur les communications militaires. Je tiens à exprimer ma gratitude à l'Université de Défense Nationale Miklos ZRINYI et particulièrement au Lt-Colonel Zoltan RAJNAI de nous donner cette année l'opportunité de présenter nos solutions adaptées aux besoins en transmissions des Postes de Commandement. La modernisation des Forces Armées entreprise en Europe, et plus particulièrement la réalisation de systèmes C4ISR, font aujourd'hui largement appel aux technologies de l'information utilisées dans l'Internet. C'est donc sans surprise que les standards issus de « l'Information Technology » sont aujourd'hui déployés dans les unités opérationnelles pour constituer un « Internet Tactique ». Le rôle de l'industrie électronique de défense est de proposer des solutions qui adaptent les standards civils aux spécificités de l'environnement militaire tactique, telles que la mobilité et les élongations, et aussi bien sûr maintenir une interopérabilité avec l'OTAN.

Missions typiques du combat terrestre

Avant d'aborder les solutions techniques voyons ensemble quels sont les besoins opérationnels du combat moderne. Voici par exemple une mission typique d'une unité de combat avec les actions élémentaires de cette mission. Parmi les actions élémentaires un certain nombre font directement appel au moyens de transmission et d'information embraqués dans les plates-formes de combat. Il s'agit en effet de transmettre des ordres, mais aussi d'acquérir et de distribuer des informations au cours de la mission, et aussi de faire partager la situation de façon à permettre un combat coopératif entre les unités tactiques.



Missions typiques en zone urbaine

L'exemple d'une mission en zone urbaine, avec des actions élémentaires un peu différentes, montre le même besoin de communiquer et d'échanger des flux d'information au cours de la mission.



Tenue de situation tactique

Le combat moderne appelle à une évolution de la doctrine au niveau tactique, et particulièrement dans le domaine des relations entre unités et la distribution de l'information. Voici par exemple les différents niveaux de commandement que l'on peut réaliser pour conduire une opération militaire. A chaque niveau de Commandement correspond un besoin particulier de connaissance de la situation tactique. Les règles de doctrine que nous allons voir sont généralement admises aujourd'hui et leur mise en œuvre se réalise avec l'arrivée des nouveaux systèmes C2: Un niveau de commandement doit avoir connaissance de la situation des unités situées deux niveaux en dessous. Par exemple la division doit connaître la situation de ses Brigades et des Bataillons de celles-ci. Un niveau de commandement doit avoir connaissance de la situation de l'unité immédiatement supérieure. Par exemple un Bataillon doit connaître la situation de la brigade à laquelle il appartient. Il doit avoir connaissance de la situation des unités de même niveau. Par exemple une Compagnie ou un Escadron doit connaître la situation des Compagnies ou Escadrons latéraux. Enfin il est souhaitable de connaître la situation des unités subordonnées des unités latérales comme nous allons le voir dans un exemple.

Tenue de situation tactique au niveau Bataillon

Appliquons ces règles de doctrine par exemple au niveau d'un Bataillon.

- Connaissance de la situation deux niveaux en dessous : donc les Compagnies du Bataillon et les Sections,

- Un niveau au dessus : donc situation de sa propre Brigade,
- Connaissance des unités latérales : dans l'exemple il s'agit de la situation du Bataillon de reconnaissance de la Brigade, d'un Bataillon blindé situé sur son flan droit, et d'un Bataillon d'artillerie qui appuie la manœuvre de la Brigade.
- Finalement il est souhaitable que le Bataillon ait une connaissance de la situation des Escadrons qui assurent la reconnaissance devant lui, des Escadrons blindés situés à sa droite, et des Batteries du Bataillon d'artillerie et tout particulièrement la situation de la Batterie qui l'appuie directement.



Remontée des positions au niveau Bataillon

La technologie aujourd'hui disponible permet de réaliser le vieux rêve de tout commandant d'une unité de combat, c'est à dire connaître en temps quasi réel la position de ses subordonnés. Dans l'exemple on voit un Bataillon dont deux Compagnies sont en mouvement vers leurs objectifs alors qu'une Compagnie reste en réserve sur sa position. Grâce à l'échange cyclique des données de position des véhicules dans le réseau du Bataillon, et grâce aux nouvelles générations de postes radio de combat, l'animation que vous avez vue est une illustration de nouveaux services disponibles en opérations militaires.

Tactical Internet (TI)

Voyons maintenant les moyens de transmissions tactiques qui permettent de satisfaire ces différents besoins opérationnels. L'approche de Thales consiste à réaliser un Internet Tactique Déployable constitué de nœud de communications qui vont desservir les Postes de Commandement. Ces Nœuds sont reliés par des liaisons hertziennes tactiques à haut débit. Et de connecter à cet Internet Tactique Déployable des réseaux Internet Tactique mobiles. Il s'agit d'assurer la continuité pour la téléphonie et les moyens C2 des Postes de Commandement statiques, avec la phonie et les moyens C2 des Bataillons.

Besoins au PC de Brigade

L'état-major au PC de Brigade met en œuvre des moyens C2, dont la mise en réseau se fait par des LAN Ethernet sécurisés, tout comme les réseaux d'entreprise. Mais avec ceci de particulier que le PC de Brigade peut être appelé à se déplacer dans l'urgence. La messagerie opérationnelle consiste aujourd'hui à transférer des données IP vers les autres Postes de Commandement, ce qui fait appel à utilisation de serveurs de messagerie tout comme dans le monde de l'Internet civil, mais avec la nécessité de joindre aussi les systèmes C2 mobiles raccordés à des radio de combat. Le commandement a bien sûr toujours un impérieux besoin de communications téléphoniques, qu'il faut satisfaire avec des interfaces radio HF et VHF CNRI. Dans l'architecture Internet Tactique Thales propose un Nœud TI de Poste de Commandement. Voyons de quoi il se compose : Comme l'état-major dispose de terminaux informatiques et de stations multimédia utilisant les technologies IP et Ethernet, le cœur d'un nœud TI de PC est constitué d'équipements LAN civils, c'est à dire un router, un commutateur Ethernet et un IPBX. De ce cœur IP partent les liaisons vers l'extérieur qui sont protégées par des équipements de chiffrement d'artère.



Dans l'architecture de Thales ces liaisons sont réalisées par des Faisceaux Hertiens à 8 Mbit/s constitué d'un équipement intérieur "Bande de Base" et d'un équipement extérieur "Radio Fréquence" avec une antenne électronique active. Ces deux équipements étant reliés par un câble à fibre optique dont la longueur peut aller jusqu'à 2 Km. Pour relier les usagers mobiles le nœud TI dispose d'un module CNRI avec une fonction "Gateway phonie" et une fonction "Gateway data". La gestion locale du nœud TI offre des fonctions de serveur d'authentification, de serveur de messagerie, de serveur web, etc.. Ceci pour le service des usagers du Poste de Commandement, qu'il s'agisse d'un LAN C2, d'applications bureautique, de téléphonie IP ou de téléphonie analogique classique. Voici un exemple de réalisation d'un nœud TI de Poste

de Commandement en version caissons transportables, en mesure d'être déployé dans un bâtiment, sous tente, ou encore dans un véhicule banalisé. Il offre tous les accès et que peut souhaiter l'état-major pour connecter ses systèmes d'information en réseau sécurisé et disposer de services téléphoniques performants. Ce module Tactical Internet de Poste de Commandement peut être bien entendu installé aussi en shelter.

Besoin en transmissions du PC de Bataillon

En ce qui concerne les besoins transmissions d'un Poste de Commandement du niveau Bataillon, en plus des liaisons vers la Brigade, ils sont de trois ordres : D'abord des besoins phonie pour le réseau de commandement interne du Bataillon. Ensuite des besoins en transmissions de données pour satisfaire la messagerie opérationnelle entre Bataillon et Compagnie ou Escadrons. Enfin, un besoin nouveau de transmission de données, il s'agit de la transmission de données cycliques comme la position des véhicules de combat. Avec le même principe que précédemment le nœud TI de PC mobile est organisé autour d'un commutateur de bord IP/Ethernet. Celui-ci permet de constituer un "Local Area System" dans le véhicule de commandement :

- qui offre un service d'interphone à l'intérieur du Poste de Commandement,
- dispose d'accès Ethernet pour raccorder le système C2 embarqué
- les flux IP sortant peuvent aller soit vers des postes de combat VHF
- ou des postes de combat HF.



Voici la réalisation matérielle du nœud Tactical Internet pour Poste de Commandement mobile

- avec le commutateur de bord SOTAS-IP
- le service interphone de bord,
- le système C2 Maestro embarqué,
- la radio de combat VHF PR4G Fastnet,
- et la radio HF TRC 3700.

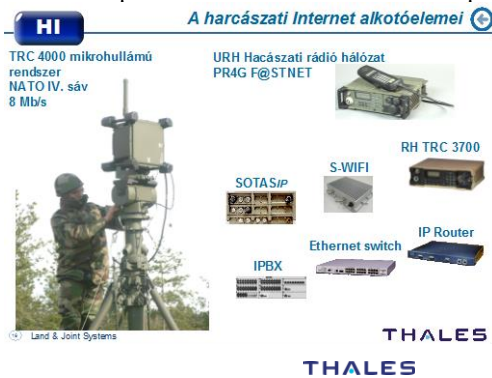
Et finalement l'intégration du nœud Tactical Internet de PC mobile dans un véhicule de commandement blindé.

Poste de Commandement tactique wireless

La technologie du commutateur de bord SOTAS-IP est compatible avec une connexion wireless COTS au standard 802.11. Thales a développé un équipement Secure-WIFI sur ce standard avec la nécessaire militarisation suivante :

- un shifting en fréquence dans la bande de 2 à 6 GHz, pour éviter d'utiliser le canal WIFI civil à 2.45 GHz.
- La puissance du composant WIFI civil limitée à 100 mWatts a été portée à 1 Watt,
- permettant une portée de plus de 1 Km en espace libre en "802.11 standard b"
- 250 mètres en "802.11 standard g".
- La connexion wireless a été sécurisée.
- Enfin cet équipement permet un réseau ad hoc point multi-points.

Voici pour conclure les briques essentielles que nous retrouvons dans les solutions statiques et mobiles de l'Internet Tactique de Thales.



**Harcászati Internet és a
vezetési pontok**

Division Land & Joint Systems

Jean-Louis DEBEURET
Defence Tactical Communications

Dr. Zoltan Rajnai – Laszlo Trembeczky
SATCOM et interoperabilité
(A Bolyai János Kutatási Ösztöndíj támogatásával)

Dans les années '70 et '80 il y a eu beaucoup de pays qui reconnaissent l'importance stratégique de l'espace et s'apprêtait à rejoindre le club des grandes puissances dotées de systèmes militaires de télécommunications par satellite. Très rapidement, l'emploi opérationnel de tels systèmes s'est avéré primordial pour les forces armées. En France, par exemple depuis 1985, date de la première mise en service opérationnelle, le système de radiocommunication utilisant un satellite répond pleinement à l'impérieuse nécessité de disposer, au profit des éléments déployés hors du territoire métropolitain et des forces à la mer, de moyens de communications sûrs, disponibles et sécurisés. C'est le seul moyen capable d'offrir en permanence et immédiatement ces liaisons théâtre-métropole et théâtre-théâtre.

Raccordé à la fois aux réseaux tactiques de zone et aux réseaux d'infrastructure, le système satellite assure le transfert des flux d'information, afin d'offrir des services de bout en bout, et participe à la conduite des opérations, tant pour le commandement, le renseignement, la mise en œuvre que pour la logistique. Apté à véhiculer à très longue distance des débits élevés, il l'aide de terrains de plus en plus compacts et faciles d'emploi, et dans des zones difficiles d'accès pour des utilisateurs isolés, le satellite constitue un outil indispensable auxquelles forces projetées ont massivement recours. L'engagement sur un théâtre extérieur ne se conçoit plus sans utilisation de moyens de communication par satellite.

Une architecture permettant une grande flexibilité

La réalisation d'un système de télécommunications par satellite est un défi qui témoigne à la fois d'une volonté d'y parvenir, de grandes compétences d'ingénierie, d'un haut niveau technologique et de ressources financières adéquates. En décidant de s'associer à France Télécom, la Défense recherchait la synergie des compétences, la mutualisation des ressources et le partage des risques. Les satellites de la famille Télécom, conçus selon cette stratégie de partenariat, tous mis en orbite avec succès, embarquent sur une même plateforme deux charges utiles, l'une commerciale spécifique à France Télécom et l'autre d'usage réservé aux militaires. Développé initialement dans un cadre géopolitique de "guerre froide", le système satellite est conçu à son origine comme un système centralisé. Il doit permettre au chef d'état-major des armées de disposer d'un moyen de communication sûr, disponible et sécurisé avec les commandants des forces déployées hors du territoire national. L'architecture retenue s'appuie sur des stations autonomes présentant des protections efficaces face aux menaces nucléaires ou chimiques. Des

échanges à l'intérieur d'une zone sont également possibles.

Pour la seconde génération, il a su anticiper certaines évolutions de besoins et, dans la plupart des cas, les prendre en compte sans bouleversement de son architecture, tout en assurant la continuité de service des fonctions existantes. Pour mieux satisfaire les besoins des forces projetées, la charge utile dispose d'une antenne "spot", déplaçable dans toute la couverture du satellite, qui permet de concentrer l'énergie rayonnée dans une zone particulière de déploiement des forces. L'augmentation du parc de stations autonomes (mobiles), à actuellement 150, parmi lesquelles de nouveaux types pour sous-marins et véhicules légers, traduit le besoin des armées de disposer d'une panoplie adaptée à un maximum de vecteurs opérationnels. Ces porteurs, apportant chacun leurs contraintes propres en termes d'intégration et d'emploi, ont nécessité des infrastructures spécifiques. Une telle diversité du parc de stations, combinée à celle des services offerts (téléphonie, télégraphie, transmission de données, etc.) requiert une très grande flexibilité pour établir, à la demande, tout type de liaison souhaité et pour reconfigurer aisément le réseau dans les meilleurs délais possibles.

Evolution du besoin opérationnel mis en évidence au cours des conflits

Au cours des dix dernières années, les télécommunications militaires ne sont pas restées à l'écart de la profonde mutation du monde de l'information. Elles ont utilisé les nouvelles technologies civiles pour offrir des services à l'identique des systèmes commerciaux, tout en préservant leurs caractéristiques et spécificités militaires. Le système satellite a aussi évolué progressivement, en tirant profit de l'expérience des derniers conflits. En 1991, la guerre du Golfe a clairement montré que seules les communications par satellite permettaient de maintenir les liaisons de commandement, lors d'opérations avec mouvements de grande élongation, alors que les systèmes classiques à base de faisceaux hertziens étaient dans ce cas moins bien adaptés. Les éléments précurseurs ou les unités agissant isolément doivent disposer également de liaisons fiables. Pour répondre à ce besoin de mobilité et de "tacticité", les armées se sont dotées, dès 1995, de stations portables.

D'autre part, l'importance du renseignement provenant en particulier des informations fournies par les systèmes d'observation spatiaux a été confirmée à cette occasion. Indispensables au niveau stratégique, elles doivent également être diffusées, souvent dans l'urgence, vers le théâtre d'opérations. Il s'agit notamment des photographies d'objectifs. Le transfert de ces données, sous forme de fichiers volumineux, nécessite des liaisons longues distances à forte capacité, que seul le satellite peut fournir. L'augmentation constatée des débits au cours des opérations en ex-Yougoslavie résulte de l'accroissement du volume des forces à desservir et des besoins opérationnels induits par la préparation et la conduite des opérations. En particulier, la mise en œuvre de

SIC (systèmes d'information et de commandement) et la desserte d'un nombre croissant d'abonnés locaux sur zone contribuent largement à cette évolution. Par ailleurs, la vidéo-conférence, qui permet d'établir un lien direct de chef à chef, est maintenant devenue un moyen de commandement irremplaçable. Enfin, il ne faut pas négliger la part des outils maintenant couramment utilisés comme la messagerie avec pièces jointes. Pour répondre à ces besoins, les forces françaises ont déployé en Bosnie et au Kosovo des stations dites "hauts-débits" reliées à la métropole avec un des liens à 2 Mbit/s.

Nécessité d'une interopérabilité avec les systèmes alliés

Alors qu'un programme satellite s'est inscrit initialement dans une démarche nationale interarmées, les opérations conduites au cours des dernières années ont mis en avant le besoin sans cesse croissant d'interopérabilité avec nos alliés. Les forces sont régulièrement appelées à opérer sous l'égide de l'ONU. Des bâtiments de la marine nationale sont intégrés dans des forces navales alliées, et les opérations majeures dans lesquelles sont engagées les forces, sont également conduites dans le cadre de coalitions multinationales. Dans de telles circonstances, il est indispensable de disposer d'interconnexions entre le système de télécommunication par satellite français et les systèmes équivalents des nations alliées. Les systèmes de télécommunications par satellites des Alliés¹⁶⁷ utilisent la gamme de fréquence SHF et les répéteurs sont de simples relais du signal. Cette conception commune constitue la première marche indispensable à l'interopérabilité. Cependant la recherche d'une interopérabilité de bout en bout est plus complexe et requiert en particulier l'utilisation de modems compatibles et d'éléments cryptographiques identiques. Elle a été mise en pratique à plusieurs reprises entre unités françaises, américaines ou espagnoles, via leurs systèmes nationaux. Pour renforcer ces possibilités, les pays participent activement aux travaux de standardisation au sein de la structure OTAN des C3. Par ailleurs, la mise en place de passerelles terrestres permet également de satisfaire le besoin opérationnel d'interconnexions. C'est ainsi que des liaisons ont été réalisées entre le système satellite français et les systèmes Skynet britannique (en bande SHF) et Fleetsatcom américain (en bande UHF). Ainsi au cours des années, le système satellite français a-t-il su s'adapter à l'évolution des besoins des armées françaises, sans profonde modification de son architecture.

A la suite de l'épuisement des réserves d'ergol, l'actuelle constellation faite de quatre satellites en a été réduite à deux en 2002 en France. Afin de garantir dans un premier temps la continuité du segment spatial, la Défense doit mettre en service un satellite de nouvelle génération début 2004 et le compléter dans les années 2006-2007.

¹⁶⁷ EU (DSCS III) - GB (Skynet 5) - OTAN (NATO IV) - France (Syracuse)I \spagne (Hispasat)
- Italie (Sieral) - Turquie (Turcsat)

Breitner Gábor

Műholdas távközlési eszközök és szolgáltatások

Műholdas távközlési eszközök és szolgáltatások

Breitner Gábor – Guards Távközlési Rt.



Kapcsolat

GUARDS Távközlési Szolgáltató Zrt.

1135 Budapest, Frangepán u. 84/B.

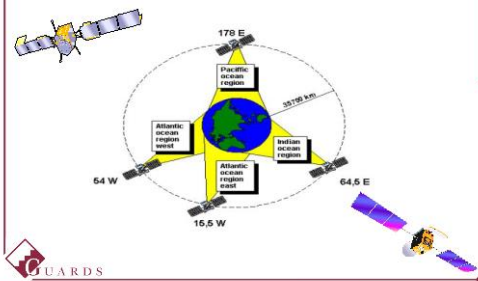
Telefon: 336-3044

Fax: 336-3049

www.guards.hu



Inmarsat műholdak



Új generációs műholdak (I-4)

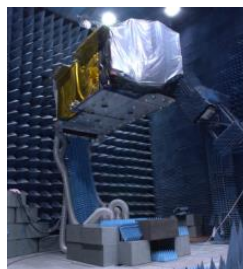


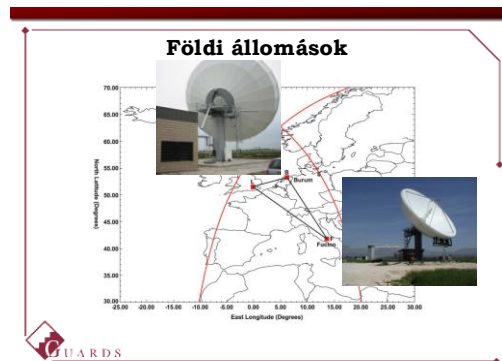
- Legfejlettebb kereskedelmi műholdak amit valaha is pályára állítottak
 - 16 x kapacitás
 - 60 x teljesítmény
- A hálózat kapacitása az igények szerint átcsoportosítható a műholdakon
- Élettartam 2023-ig garantált
- Sikeres pályára állítások
 - F1: 2005.03.11.
 - F2: 2005.11.08.



Inmarsat I4 műhold

A világ legnagyobb távközlési műholdja





Inmarsat BGAN 30 mp-ben



Az első műholdas szolgáltatás amelynél:

- Nagysebességű adatátvitel (max. 492 kbit/s)
- hanghívás
- egy időben használható
- egyetlen kompakt eszközzel
- igény szerint garantált adatátviteli sebességgel
- globálisan elérhető hálózattal



BGAN telefon szolgáltatás

Vonalkapcsolt hang hívások

- Földi vonal minőségű hang (4kbps)
- Hívás indítás és fogadás
 - Földi vonalas hálózat
 - Mobil (GSM) hálózat
 - BGAN és egyéb műholdas hálózat

Kiegészítő szolgáltatások

- Audió tartozékok széles választéka



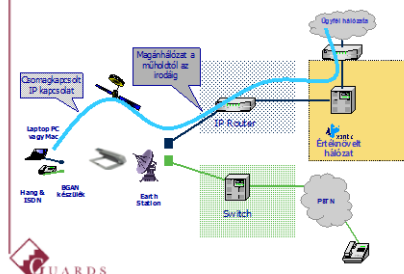
Hangposta szolgáltatás a földi állomáson

Vonalkapcsolt ISDN (Adat/Hang/Fax)

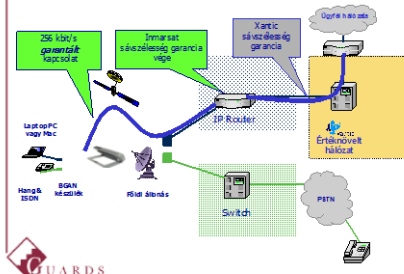
- Terminál függő szolgáltatás
- Egy **64 Kbps** ISDN csatorna **készülékenként**
- Bármely ISDN alkalmazással kompatibilis szolgáltatás
 - titkosító eszközök (STE, AES)
 - műsorszórás



Üzleti hozzáférés



Garantált hozzáférés



Vigh Levente

Információvédelmi szempontok és a WiMAX alkalmazási lehetőségei
(Részlet a WiMax és az információvédelem című tanulmányból)

A Magyar Honvédség stacioner hírendszere nagyjából megfelel a kor színvonalának: a döntéshozatali helyeken magas szintű az informatikai és kommunikációs ellátottság, a gerinchálózat pedig az elmúlt évtizedben lett korszerűsítve. Nem indokolt továbbá a meglévő vezetékes rendszer kiváltása vezeték nélküli hálózattal, hiszen az objektumok nagy részében már strukturált hálózat van, a többiben pedig a közeljövőben kerül kiépítésre. A tábori hírendszerben jelenleg alkalmazott közepes távolságú összeköttetési módok (mikrohullám, rádió) azonban nem csak a polgári életben alkalmazott technológiákhoz képest, hanem már önmagukban is elavultnak számítanak, nem alkalmasak a jelenlegi igények kiszolgálására. Továbbfejlesztésük nem lehetséges, ezért szükség van a kiváltásukra. A modern harcvezetés elengedhetetlen része az informatikai és kommunikációs eszközök széles körű alkalmazása. A parancsnoki döntéshozatal nem csak a modern üzenettovábbítási formák (SMS¹⁶⁸, e-mail, stb.) segítik elő, hanem a harcmezőről érkező, legváltozatosabb információk (képek, videók, szenzorok jelei, stb.) megjelenítése is fontos. A mai hadviselés egyik kulcseleme a *real-time* adatszolgáltatás, vagyis az információk valós idejű továbbítása. Ezek az új döntéstámogató eszközök napról napra nagyobb hatékonysággal segítik a parancsnoki munkát, ennek ára viszont a nagyobb kommunikációs kapacitás-igény.

Véleményem szerint a WiMAX – megfelelő biztonsági kiegészítésekkel – megoldást jelenthet a Magyar Honvédség tábori hírendszérének modernizálására. Az eszközök tábori alkalmazása a szélsőségesebb környezeti és fizikai hatások miatt (por, sár, csapadék, hőmérséklet) nagyban eltér a védett objektum belülről, ami kihatással van mind az eszközök kialakítására (robosztusabb, erősebb kivitel), mind az alkalmazási módra, mind pedig az üzemeltető- és felhasználói állományra. A megnövekedett kockázat miatt (ellenséges felderítés, telepítési körülmények, stb.) azonban minden lehetséges eszközzel, szabályzóval, eljárással törekedni kell a minél magasabb szintű biztonságra.

A tábori elhelyezés körülményei nagyon változatosak lehetnek az alakulat nagyságától, a művelet helyszínétől (hazai, vagy külföldi) és jellegétől (támadás, védelem, békefenntartás, stb.), a terepviszonyoktól és sok minden mástól függően. Éppen ezért nem lehet általános szabályokat lefektetni úgy, mint egy védett objektumban alkalmazásra kerülő CIS, vagy eszköz esetén. Sem a nemzeti, sem a szövetségi doktrínákban, szabályzóknak nincs konkrét utasítás a fizikai biztonság megszervezésére. Abban viszont mindkét megfogalmazás egyet ért, hogy a telepítési helyszínt (vezetési pont, gépjármű cso-

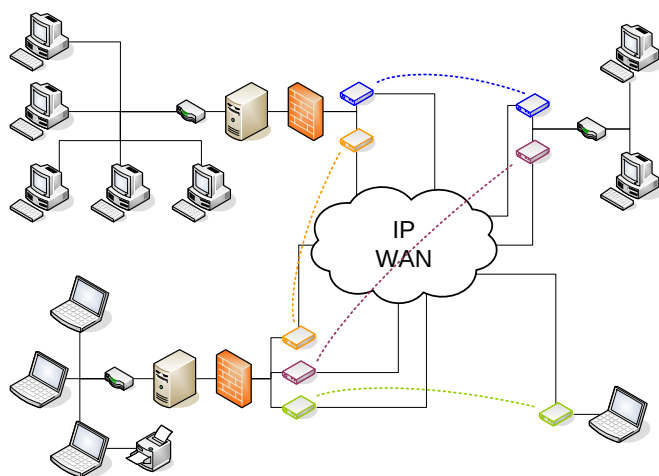
¹⁶⁸ Short Message Sending – Rövid szöveges üzenet küldés

port, stb.) folyamatos, 24 órás őrzéssel kell biztosítani és ezen felül minden lehetséges módon védeni kell a titkosító eszközöket és a minősített információt kezelő berendezéseket. NATO terminológiában létezik egy ún. CCI¹⁶⁹ kifejezés, mely olyan eszközöket takar, melyek megfelelő kezelés esetén képesek titkosítás végrehajtására, de önmagukban nem hordoznak minősített információt. CCI-nak minősül egy kulcsolatlan rejtjelző berendezés, vagy egy üres elektronikus kulcstár. Ezeket szintén őrizni kell, de nem olyan szigorú feltételek között, mint egy kulccsal ellátott berendezést. (Egy bekulcsolt berendezés minősítési szintje megegyezik a betöltött kulcs minősítési szintjével, vagy annál eggyel magasabb.) A személyi biztonság területén van a legkisebb különbség a tábori és a védett objektumon belüli alkalmazás között. Az állomány, az előzetes kiválasztás során átesett a megfelelő átvilágításon, így azt nem szükséges megismételni. Fokozottabb odafigyelést az ellenséges beszivárgó erők, felderítők igényelnek. Tábori alkalmazás során a tevékenység jellegétől függően másféle jellegű és mennyiségű ügyirat, információhordozó keletkezik. Tülnyomó többségben térképek, harcmozgási tervek, felderítési adatok, stb. keletkeznek. Kevesebb a magas minősítési szintű információ, viszont több alacsony minősítésű anyag születik. Ezeket ugyanúgy továbbítani, tárolni és dokumentálni kell, majd meg kell semmisíteni. Szintén fokozottabb odafigyelést igényelnek az ellenséges tevékenység miatt.

A fizikai környezet talán az informatikát érint legkevésbé: COMPUSEC szempontból a tábori alkalmazás szinte megegyezik a stacioner alkalmazással. Ugyanúgy szükség van a megfelelő védelmi rendszerek (tűzfalak, szűrők, vírusirtók, stb.) alkalmazására, valamint a hozzáférési jogosultságok szabályozására. COMSEC szempontból a tábori körülmények leginkább a kulcsmenedzsment szempontjából támasztanak kihívást. Akárcsak napjaink számítógép hálózatai, a WiMAX is IP protokollt használ. Ez a világon az egyik legelterjedtebb protokoll, aminek előnyei és hátrányai is vannak. Elterjedtsége és egyszerűsége jelenti ráadásul mindkettőt. Megfelelő konfigurálás esetén számos védelmi funkció áll rendelkezésre, amelyekkel biztosítható egy elfogadhatóan alacsony szintű kockázat. Amennyiben viszont maradnak védtelen pontok, az olyan támadási felületet jelent, ami beláthatatlan következményekkel járhat. Az informatika körébe tartozó védelmi rendszereken kívül (tűzfalak, vírusvédelmi szoftverek, stb.) fontos szerep hárul a titkosító berendezésekre. Léteznek különböző típusú titkosító algoritmusok, melyek különböző kulcsrendszereket (egy-, vagy kétkulcsos), kulcshosszokat alkalmaznak. Jelen pillanatban is többféle ilyen eszköz van rendszeresítve az MH-ban. Annak érdekében, hogy egy újonnan bevezetésre kerülő eszköz vagy rendszer a jelenlegi rendszerekkel képes legyen együttműködni, célszerű már meglévő titkosító eszközt alkalmazni. Már csak azért is, mert egy új eszköztí-

¹⁶⁹ *Controlled Cryptographic Item* – Ellenőrzött titkosító tárgy

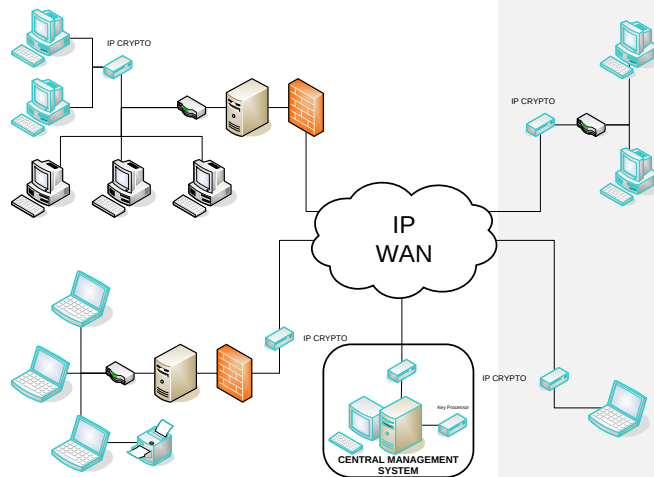
pus bevezetése a hatalmas költségek mellett alapos és hosszadalmas akkreditálási procedúrát, tesztelést von maga után, és még így is jelent biztonsági kockázatot. Ajánlott továbbá olyan eszközt alkalmazni, amely nemzetközi, szövetségi műveletek esetén biztosítja a kompatibilitást, adott esetben az interoperabilitást az együttműködők irányában. Az MH-ban jelenleg is van rendszeresítve olyan korszerű IP alapú titkosítást végző eszközük, amely ezeknek a követelményeknek megfelel. Az eszközöket és pontos paramétereiket a hatályos jogszabályok miatt jelen munkában nevesíteni nincs lehetőség, de bizonyos funkciók – melyek általánosan jellemeznék egy modern titkosító berendezést – ismertethetőek. A fejlett berendezések már nem az összeköttetési vonalakat, hanem magát az információt titkosítják. Régen minden egyes vonalhoz volt egy titkosító berendezés rendelve, ami jelentősen megnövelte az alkalmazandó eszközök számát, ráadásul a hozzáférés jogosultság kizárólag a szerverek beállításától függött.



9. ábra: Vonal titkosítás

Egy modern IP rejtjelző berendezés képes az egyes csomagokat titkosítani, így nincs szükség a vonalankénti titkosításra, hiszen az IP fejrészben ott van a címezés. Ugyanakkor az így címzett csomagok elfoghatóak és módosíthatóak, vagy akár feltörhetőek is, ezért a mai berendezések már nem csak a csomag hasznos terhet (vagyis a benn tárolt információt) titkosítják, hanem az IP fejrészt is. Az eszköznek van egy be- és egy kimeneti oldala, és ezek más-más IP-címmel rendelkeznek. Ezáltal kivédhető a csomagok szándékos elfogása, hiszen semmi nem utal sem a feladóra, sem a címzettre. A védett (nyílt) oldali címet *red*-oldali címnek, míg a kimeneten megjelenő (titkosított) címet *black*-

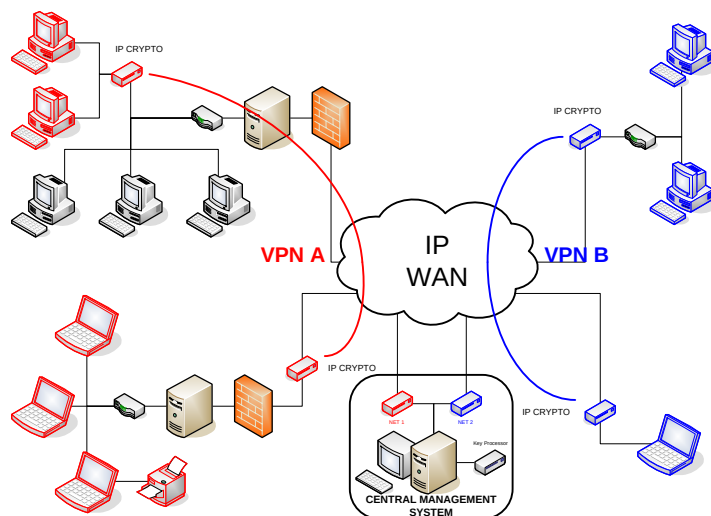
oldali címnek nevezzük. Így lehetőség nyílik a hozzáférés kontroll magasabb szintre emelésére, hiszen csak azok a számítógépek férhetnek hozzá a minősített információkhoz, amelyek a berendezés *red* oldalán vannak. Ezek a terminálok viszont a külső hálózat felől láthatatlanok minden berendezés számára, amelyek nincsenek ellátva a megfelelő (azonos algoritmussal és kulccsal dolgozó) IP crypto eszközzel. Az IP crypto berendezés számára nem mindegy viszont, hogy milyen eszköz, vagy eszközök vannak a *red*-oldalán. A crypto berendezéseket egy menedzsment központ (CMS¹⁷⁰) vezérli, és ez tárolja a védett hálózatban szereplő terminálok adatait.



10. ábra: IP titkosító eszközük + CMS

A központban van két további crypto berendezés, melyek közül az egyik a központi szerver és a hálózat között helyezkedik el, feladata a kódolt információ dekódolása és a szerver védelme a közvetlen hozzáféréstől. A másik eszköz feladata a kulcsok gyártása. A CMS képes arra, hogy két, egymástól független hálózatot kezeljen úgy, hogy azok egymást ne láthassák, vagyis virtuális magánhálózatot (*Virtual Private Network*) alkossanak.

¹⁷⁰ Central Management System

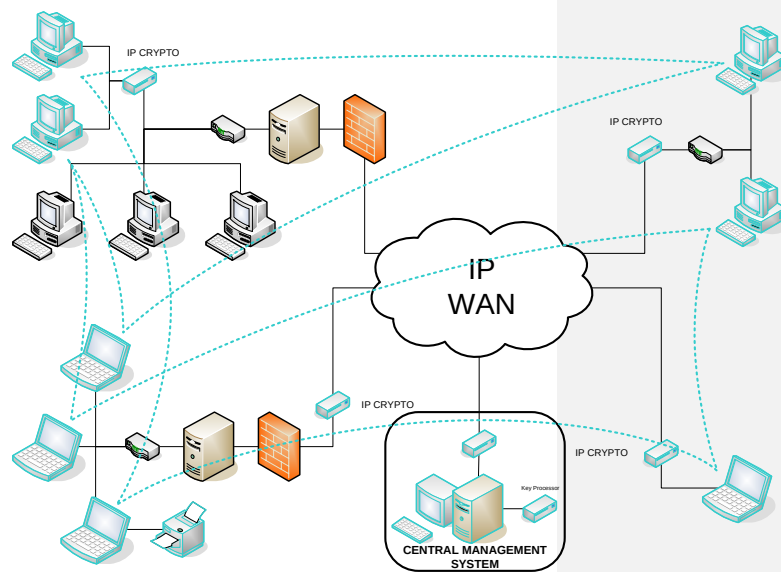


11. ábra: Virtuális magánhálózat (VPN)

Ebben az esetben a központhoz nem egy, hanem két crypto berendezés csatlakozik, melyek külön-külön kapcsolódnak a nyilvános IP hálózathoz. További funkció a hozzáférés-vezérlés (ACM¹⁷¹), melynek lényege, hogy a központ felhasználói terminálokra lebontva képes megszabni/engedélyezni, hogy ki kivel léphet kapcsolatba (kivéve a fent említett esetben, amikor szerver mögött vannak a számítógépek). Ezzel az eljárással (kiegészítve természetesen a megfelelő jelszavas védelemmel) maximalizálható a biztonság, és a *need-to-know* elv érvényesülése. A központban tárolt hozzáférés-vezérlési információ bármikor megváltoztatható. Ha például egy alhálózatban felmerül a kompromittálódás gyanúja, a központban azonnal letiltható a crypto berendezés, így a védett hálózat többi elemével megszűnik a kapcsolata. Mivel a fejlett IP crypto rendszer nem a vonalat, nem a bitfolyamot, hanem az egyes IP csomagokat titkosítja, ezért lényegtelen, hogy milyen átviteli (fizikai) közegen folyik a kommunikáció. A berendezések szabvány csatlakozóval vannak felszerelve, melyhez megfelelő adaptert illetve kiválaszthatjuk, hogy UTP¹⁷², vagy optikai kábelon kívánjuk továbbítani az információt. Ennek megfelelően a transzport hálózat akár WiMAX is lehet, vagy vegyes topológiát is alkalmazhatunk.

¹⁷¹ Access Control Management

¹⁷² Unshielded Twisted Pair – árnyékolatlan csavart érpár



12. ábra: Hozzáférés-vezérlés (ACM)

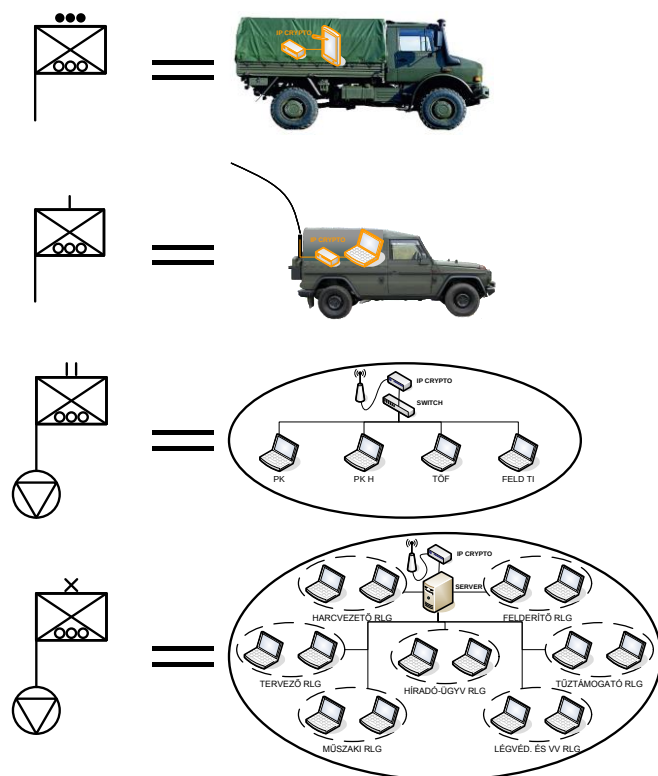
A WiMAX alkalmazási lehetőségei

A 802.16 szabványcsalád számos lehetőséget kínál mind a civil, mind a katonai alkalmazás számára. Nagy átviteli sebessége (max 280 Mbps/bázisállomás [3]) és PMP üzemmódja egyaránt alkalmassá teszi gerinc-hálózati-, és mint *last mile*-elem, vagyis több felhasználót kiszolgáló bázisállomás felhasználásra. Adaptív antenna rendszer alkalmazásával jelentősen csökkenthető felesleges kisugárzás, valamint a terepviszonyokból adódó lefedettség-egyenetlenség. A MAC¹⁷³ réteg által biztosított kapcsolódási felület az IP és ATM¹⁷⁴ hálózatokhoz, átalakítók vagy kapcsolórendszerek nélkül teszi lehetővé a stacioner hírrendszerrel való összekapcsolást.

Az alkalmazási lehetőségek egy elméleti szervezeti felépítést tartalmaznak, melyek nem feltétlenül takarják az MH-ban jelenleg rendszeresített felépítést. Az alegységek vezetési pontjain szereplő berendezések a jelenlegi szervezési elvek alapján lettek felvázolva, de szintén nem feltétlenül felelnek meg a rendszeresített eszközöknek. A következő alfejezetekben bemutatásra kerülő ábrák értelmezéséhez a 13. ábra nyújt támpontot:

¹⁷³ Media Access Control – közeghozzáférés vezérlés

¹⁷⁴ Asynchronous Transfer Mode – aszinkron transzfer móód

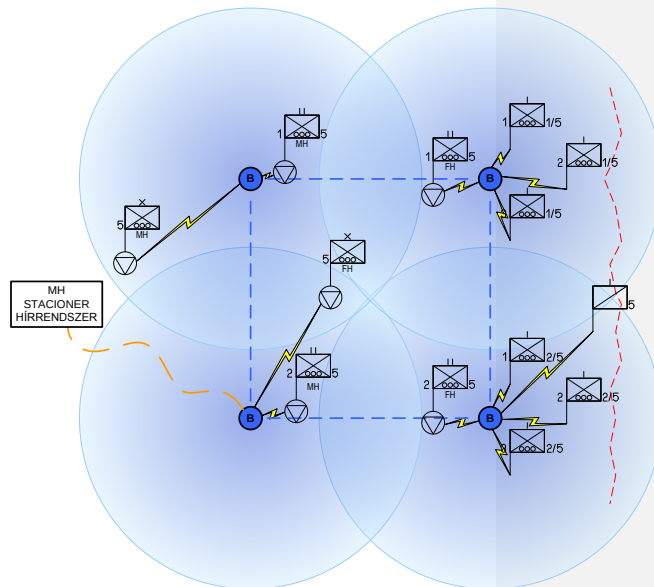


13. ábra: Alegységek és eszközeik – [10] felhasználásával

WiMAX alkalmazása rácsponti hálózatként

A WiMAX által elérhető gyakorlati lefedettség körkörös antenna esetén, jó terep- és időjárási viszonyok esetén nagyságrendileg 50 km sugarú körnek felel meg. Ez természetesen a maximális távolság, átlagosan ezért ennél kevesebbel kell számolni. Adaptív modulációt és szektorsugárzókat (pl. $6 \times 60^\circ$) alkalmazva mintegy 25-35 km-es sugarú körben biztosítható nagy sáv-szélességű hozzáférés. Ennél fogva a rendszer alkalmas lehet a jelenlegi rácsponti rendszer kiváltására, ráadásul a felcsatlakozó eszközöknél nem szükséges nagy teljesítményű mikrohullámú állomások alkalmazása. A rácsponti alkalmazást a 14. ábra mutatja. Az ACM megfelelő beállításával természetesen szabályozható, hogy melyik állomás kit érhesse el, úgy mint egy rádióforgalmi rendszer esetén. Például egy századparancsnok az előljáró zászlóalj vezetési ponttal, a szomszédos századparancsnokokkal, és adott esetben – a

zászlóalj vezetési pont kiesése esetén – a dandár vezetési ponttal tarthat kapcsolatot. A QoS funkciónak köszönhetően beállítható, hogy milyen típusú üzenetek (hang, kép, adat, stb.) élvezzen előnyt a továbbításban akkor, amikor nincs megfelelő sávszélesség az összes adat azonnali továbbításához.



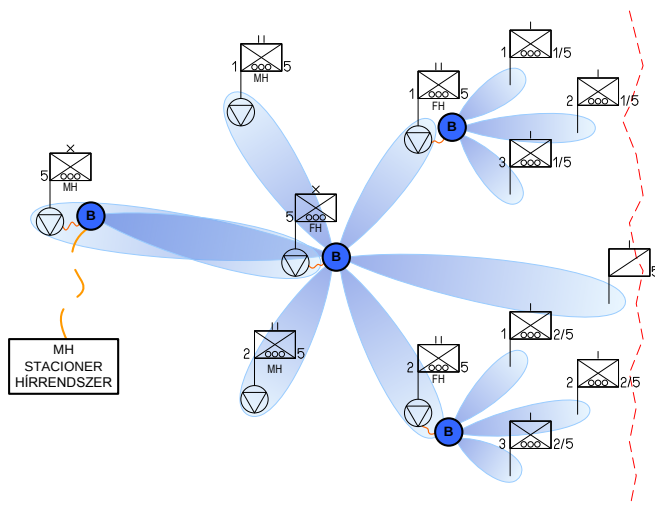
14. ábra: WiMAX alkalmazása rácsponti rendszerként

Igény esetén a központi menedzsment rendszerben a tábori és a stacioner hírendszerek szerepelhetnek egy hálózaton belül is, vagy két külön virtuális magánhálózatként, egymás számára láthatatlanul. Bármelyik megoldást alkalmazzuk, mindkét rendszer hálózat-felügyelete biztosított. Amennyiben a két hírendszert egymástól fizikailag teljesen elkülönítve kell kialakítani, akkor két menedzsment központ felállítása szükséges, ami jelentősen megnöveli a költségeket.

Bázisállomás a vezetési pontokon

Amennyiben a terep- és időjárási viszonyok nem teszik lehetővé, vagy kerülendő a felesleges kisugárzás, adaptív antennarendszerek alkalmazásával lehetőség nyílik jól irányított, szűk eredő iránykarakterisztikájú nyalábok formálására. Ebben az esetben viszont célszerű a bázisállomásokat a vezetési pontokhoz közel (párszáz méteres távolságra) elhelyezni. Ehhez optikai kábel alkalmazása javasolt, kerülendő a felesleges kisugárzást, felderíthetőséget és lehallgathatóságot. [9] Ezzel növelhető a bázisállomások felügyelete, és egy-

ben a kezelőállomány létszáma is csökkenthető. Az antennák fázisvezérlésével követhetőek a mozgásban levő eszközök, így biztosítható ugyanaz a szolgáltatásminőség, mintha körkörös lefedettségű területen mozognának. Ha viszont ellenséges területre érnek, csak a szükséges irányban történik kisugárzás, így csökken a kompromittálódás veszélye. Az ACM-ben definiált jogosultságok, valamint a QoS¹⁷⁵ beállítások természetesen ez esetben is érvényesek.

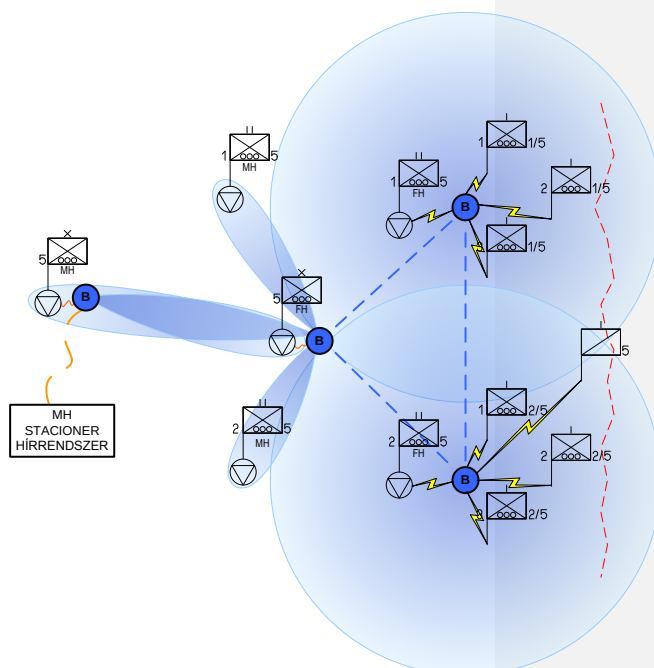


15. ábra: Bázisállomás a vezetési pontokon

Vegyes topológia

Ha a terepviszonyok, vagy az alkalmazási mód, a feladat jellege úgy követeli meg, rugalmasan alkalmazható a két rendszer ötvözte is. Ha például a frontvonal közelében a szokásosnál több különálló eszközt akarunk működtetni, viszont a fő vezetési pontok nagyobb távolságra helyezkednek el, a 16. ábra szerinti megoldás is alkalmazható.

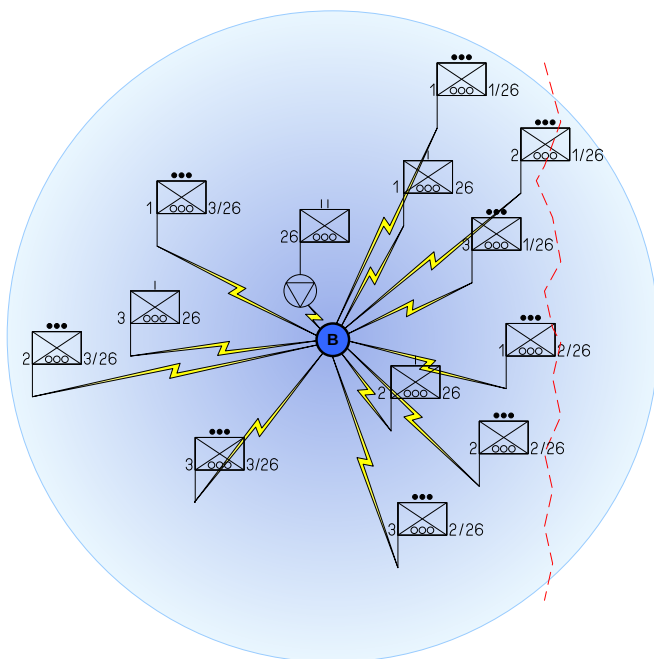
¹⁷⁵ Quality of Service – szolgáltatás minőség



16. ábra: Vegyes topológia

Önálló zászlóalj, vagy kisebb alegység kiszolgálása

Előfordulhatnak olyan esetek, amikor nem egy teljes dandár, hanem csak egy zászlóalj, vagy annál kisebb alegység kerül bevetésre. Ilyen lehet például egy katasztrófavédelem, de egy külföldi misszió is. Ezekben az esetekben a kirendelt, kiküldött erők viszonylag nem túl nagy területen, pár négyzetkilométeres körzetben helyezkednek el. A teljes szintű vezetettség érdekében akár minden járművet fel lehet szerelni WiMAX adóvevővel – és természetesen titkosító berendezéssel. Egy bázisállomás nagyságrendileg 20 felhasználói terminált tud kiszolgálni, ezért elegendő mindössze egyetlen ilyen berendezés telepítése. Ez (főleg egy külföldi misszió esetén) jelentősen csökkenti a költségeket. Amennyiben mégis nagyobb mennyiségű felhasználót kellene kiszolgálni, ez a kapacitás növelhető, méghozzá sektorsugárzók alkalmazásával. Ez 120°-os, 3 szektoros kialakítás esetén akár 60 felhasználót, 60°-os, 6 szektoros esetén akár 120 felhasználót jelent!



17. ábra: Önálló zászlóalj kiszolgálása

Következtetések

A fent bemutatott rendszerek, eszközök eljárások összegzéseként kutatásom során a következő megállapításokra jutottam:

1. A WiMAX a XXI. század elejének egyik legfejlettebb rendszere, mely nagy sávszélességű, vezeték nélküli hozzáférést biztosít LOS, NLOS környezetben, fix, nomád, mobil, vagy nagy sebességgel mozgó eszközök részére. Fejlett technológiája révén rugalmasan alkalmazható különböző topológiákban, akár körkörös (360°-os, vagy többszektoros), akár irányított karakterisztikájú lefedéssel.
2. Mivel a WiMAX szabványos kapcsolódási felületet biztosít mind az IP, mind az ATM protokoll részére, tökéletesen illeszthető a meglévő infokommunikációs rendszerekhez, legyen szó polgári, vagy katonai hálózatról.
3. A WiMAX napjainkban is fejlődő technikai rendszer, mely rejthet még magában kiaknázatlan lehetőségeket, így előremutat a későbbi fejlesztések felé. A WiMAX Fórum gyártók sorát tömöríti, ami garan-

ciát jelent a szabványosságra, az interoperabilitásra, és az olcsóbb fogyasztói árra.

4. Bár a WiMAX alapvetően polgári szabvány, az 5GHz-es NATO IV-es sáv is a definiált frekvenciák között szerepel, ezért katonai alkalmazása is lehetséges.
5. A 802.16 szabvány ugyan tartalmaz információvédelmi előírásokat, azok szintje azonban önmagában nem biztosít megfelelő védeltséget a katonai alkalmazás során továbbítandó minősített információk számára, ezért kiegészítő eszközöket kell alkalmazni.
6. A Magyar Honvédségben jelenleg is üzemelő, fejlett IP titkosító eszközrendszer alkalmazásával a WiMAX biztonságosan használható katonai célokra.
7. A MH-ban jelenleg rendszeresített tábori híradó eszközök a kor színvonalának, kihívásainak nem, vagy csak korlátozott mértékben felelnek meg.

A fentiek alapján úgy vélem, hogy a WiMAX, a dolgozatban említett biztonsági kiegészítésekkel, alkalmas lehet az előregedett technikai eszközök kiváltására, a MH tábori hírendszerének a kor színvonalának megfelelő kiszolgálására, későbbi bővítések, fejlesztések költség-hatékony implementálására.

Dr. Dárdai Árpád

Biztonsági és Diszpécser Rádiótelefon rendszerek

Biztonsági és Diszpécser Rádiótelefon rendszerek. A TETRA és a GSM-R rendszer

Dr. Dárdai Árpád
okleveles villamos szakmérnök

ZMNE, Kommunikáció 2006.

Budapest, 2006. október 25.

Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

1

TETRA Nemzetközi elterjedtsége

A TETRA alkalmazása tovább nő világszerte. Példák a létesítési szerződésekre az utóbbi időkből:

- ◆ Argentína (belügyminisztérium)
- ◆ Belgium (tűzoltóság)
- ◆ Brazília (katonaság, tűzoltóság, rendőrség)
- ◆ Kína (biztonsági szervek, rendőrség)
- ◆ Írország (rendőrség)
- ◆ Németország (BMW)
- ◆ Korea (biztonsági szervek, kormányzati célok, különféle nemzeti intézmények)
- ◆ Hollandia (rendőrség)
- ◆ Nigéria (fővárosi alkalmazások és repülőtér)
- ◆ Szlovénia (belügyminisztérium, többek között a schengeni határok felügyelete, védelme)
- ◆ Spanyolország (rendőrség, tűzoltóság, polgári védelem és más biztonsági szervek, madridi és más repülőterek)
- ◆ Venezuela (rendőrség)
- ◆ Magyarország (rendőrség, határőrség, tűzoltóság, katasztrófa védelem, stb.)

Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

4

Diszpécser rádiótelefon rendszerek kialakulása. Fejlődés a TETRA felé

- ◆ Egyszerű rádiótelefon rendszerek
- ◆ Üzem módok, rendszer típusok:
 - ◆ szimplex, félduplex, duplex átvitel
 - ◆ egyfrekvenciás, kétfrekvenciás használat
 - ◆ egyszeres lefedés, többszörös lefedés
 - ◆ analóg és digitális átvitel és rendszerek
- ◆ Nyilvános és nem nyilvános diszpécser rádiótelefon rendszerek (PMR, PAMR)
- ◆ Európai nyilvános diszpécser rádiótelefon rendszerek (EPSN) és megoldások:
 - ◆ MPT1327, TETRA, TetraPol, GSM-VPN, -CUG, GSM-Pro, GSM-R, ...

Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

7

Diszpécser hálózat típusok

- ◆ PMR (Private Mobile Radio)
- ◆ PAMR (Public Access Mobile Radio)
- ◆ Mi a különbség?



Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

8

A TETRA kialakulásának állomásai

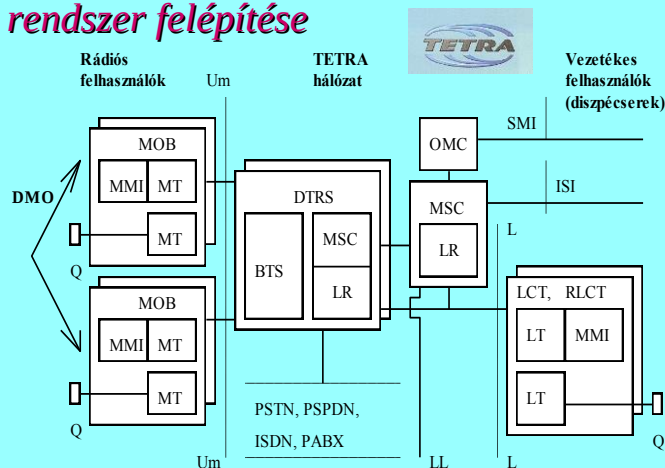
- ◆ 1989: Mobile Digital Trunked Radio System (MDTRS) kialakulása
- ◆ 1990-es évek elején: TETRA Trans European Trunked Radio megjelenése
- ◆ 1990-es évek közepe, névváltozás: TETRA, Terrestrial Trunked Radio
- ◆ 1995: az ETSI keretében kidolgozták és elfogadták a TETRA AIR interfészt
- ◆ 1996: TETRA létesítési szerződések megjelenése
- ◆ 1997: TETRA rendszerek üzembe helyezése
- ◆ 2000: TETRA Release 2 project elfogadása az ETSI keretében
- ◆ 2004-ben és utána egyre több TETRA rendszer létesítéséhez előkészületek, ill., rendszerek létesítése

Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

9

A TETRA nyilvános diszpécser rádiótelefon rendszer felépítése



Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

11

A TETRA hívások viszonylatai

- ◆ Hívás kezdés és befejezés saját hálózaton
- ◆ Közvetlen üzemmódú hívások
- ◆ Hívás kezdés és befejezés különböző hálózatokon
- ◆ Hívások a TETRA és egy alközpont (PABX) között
- ◆ Hívások a TETRA és TETRA, PSTN/ISDN és GSM között (E.164)

Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

16

A TETRA DMO szemléltetése



Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

21

TETRA TEDS bruttó adatátviteli sebesség (kbit/s) 4 időrés használatával

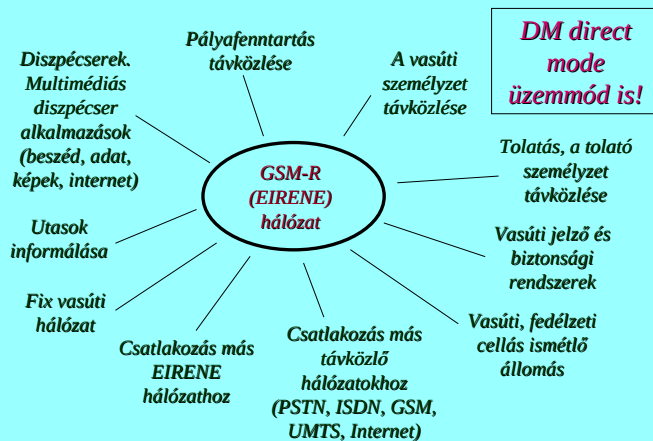
Csatorna típus→ ↓ Moduláció	25 kHz	50 kHz	100 kHz	150 kHz
$\pi/4$ DQPSK	36			
$\pi/8$ D8PSK	54			
4-QAM	38	77	154	230
16-QAM	77	154	307	461
64-QAM	115	230	461	691

Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

29

A GSM-R főbb csatlakozásai



Dárdai, 2006. október 25.

ZMNE, Kommunikáció, 2006.

35